EXHIBIT 1

US006624750B1

(12) **United States Patent**
Marman et al.

(10) **Patent No.: US 6,624,750 B1**
(45) **Date of Patent: Sep. 23, 2003**

(54) **WIRELESS HOME FIRE AND SECURITY ALARM SYSTEM**

(75) Inventors: **Douglas H. Marman**, Ridgefield, WA (US); **Kai Bang Liu**, Beaverton, OR (US)

(73) Assignee: **Interlogix, Inc.**, Tualatin, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/831,425**

(22) PCT Filed: **Oct. 6, 1999**

(86) PCT No.: **PCT/US99/23386**

§ 371 (c)(1), (2), (4) Date: **May 7, 2001**

(87) PCT Pub. No.: **WO00/21053**

PCT Pub. Date: **Apr. 13, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/103,432, filed on Oct. 6, 1998.

(51) **Int. Cl.**[7] **G08B 29/00**

(52) **U.S. Cl.** **340/506**; 340/539; 340/531; 340/825.36; 340/825.49

(58) **Field of Search** 340/506, 539, 340/531, 825.36, 825.49, 511

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,363,031 A	12/1982	Reinowitz	340/539
4,559,526 A	12/1985	Tani et al.	340/539
4,641,127 A	2/1987	Hogan et al.	379/40
4,652,859 A	3/1987	Van Wienen	340/503
4,801,924 A *	1/1989	Burgmann et al.	340/521
4,812,820 A	3/1989	Chatwin	340/518
4,855,713 A	8/1989	Brunius	340/506
4,994,787 A	2/1991	Kratt et al.	340/505
5,132,968 A	7/1992	Cephus	370/94.1
5,159,315 A	10/1992	Schultz et al.	340/539
5,319,394 A	6/1994	Dukek	348/148

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

GB	2222288	2/1990	G08C/17/00
GB	2319373	5/1998	H05Q/9/00
WO	9403881	2/1994	G08B/25/10

OTHER PUBLICATIONS

"Security For The Future, Introducing 5804BD—Advanced two–way wireless remote technology", Advertisement, ADEMCO Group, Syosset, NY, circa 1997.

"WLS906 Photoelectric Smoke Alarm", Data Sheet, DSC Security Products, Ontario, Canada, Jan. 1998.

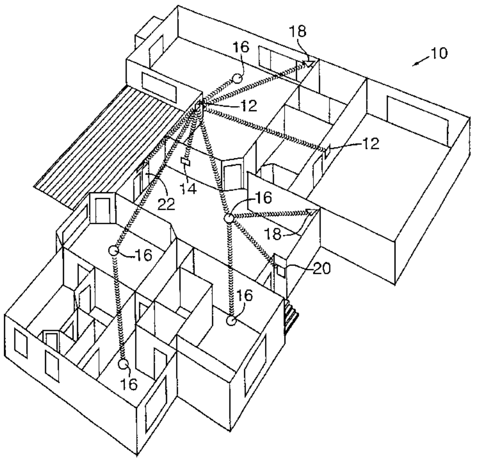
"Wireless, Battery–Powered Smoke Detectors", Brochure, SafeNight Technology, Inc. Roanoke, VA, 1995.

Primary Examiner—Daryl Pope
(74) *Attorney, Agent, or Firm*—Stoel Rivers LLP

(57) **ABSTRACT**

A wireless alarm system (**10**) employs two-way transceivers (**32, 60**) in a network of smoke detectors (**16**), a base station (**12**), and other sensors. A keypad (**14**) is not needed because the system is reset by pressing a Test/Silence button (**66**) built into every detector or sensor. A siren is also eliminated because a sounder (**64**) in every detector sounds an alarm when any sensor is triggered. This is possible because every detector includes a transceiver that can receive alarm messages from any other detector. AC power wiring is also eliminated because the base station and sensors are battery powered. Only a telephone connection (**48**) is needed if the system is to be monitored. In apartments or dormitory installations, smoke detectors in one apartment relay alarm messages to the next apartment, and onto the next, and so on, to a centralized base station for the entire facility. The centralized base station can be located in an apartment manager's office for immediate notification of an alarm, improper smoke detector operation, low or missing battery indications, and dirty smoke detector indications. The two-way wireless alarm system can save many lives in apartments, where smoke detectors batteries are often depleted or removed.

31 Claims, 6 Drawing Sheets



U.S. PATENT DOCUMENTS

5,465,081	A	11/1995	Todd	340/825.05
5,486,812	A	1/1996	Todd	340/539
5,578,989	A	11/1996	Pedtke	340/539
5,587,705	A	12/1996	Morris	340/628
5,630,216	A	5/1997	McEwan	455/215
5,731,756	A	3/1998	Roddy	340/539
5,914,655	A	6/1999	Clifton et al.	340/506
5,955,946	A	9/1999	Behesti et al.	340/506
5,959,528	A	9/1999	Right et al.	340/506

* cited by examiner

FIG. 1

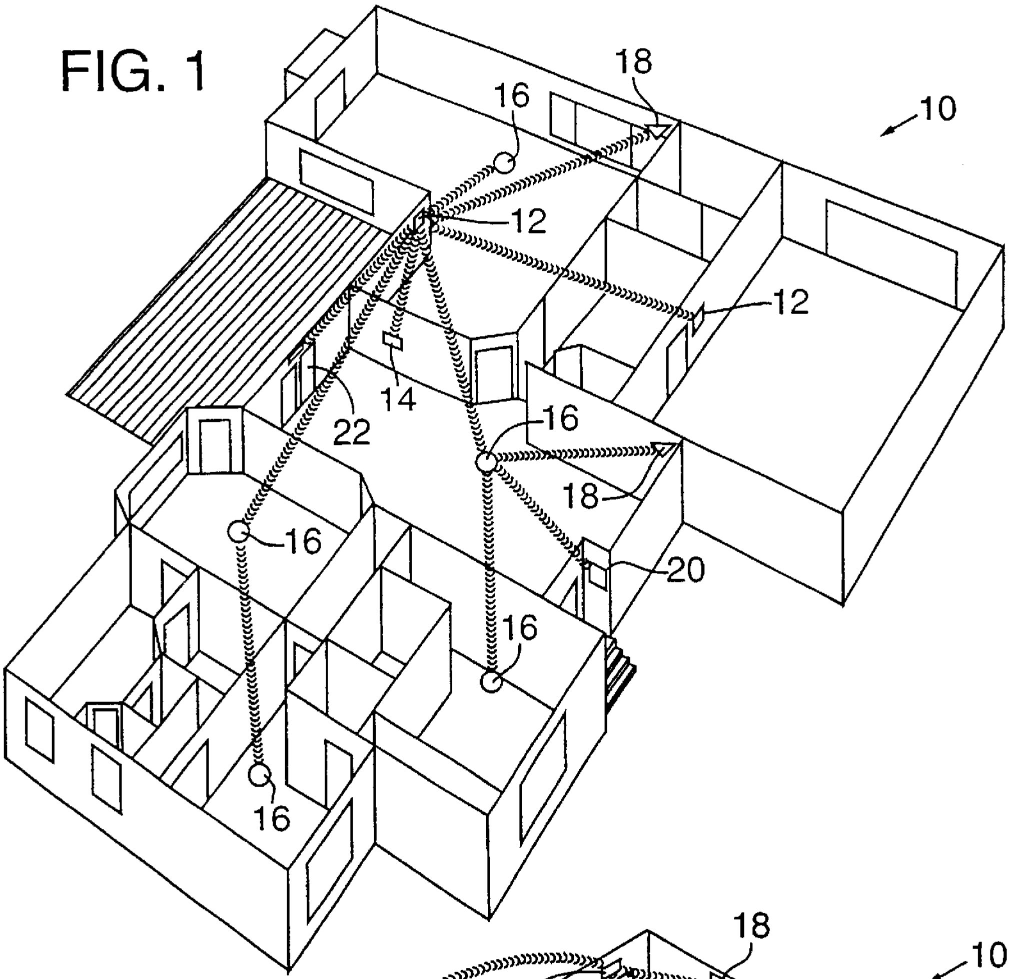
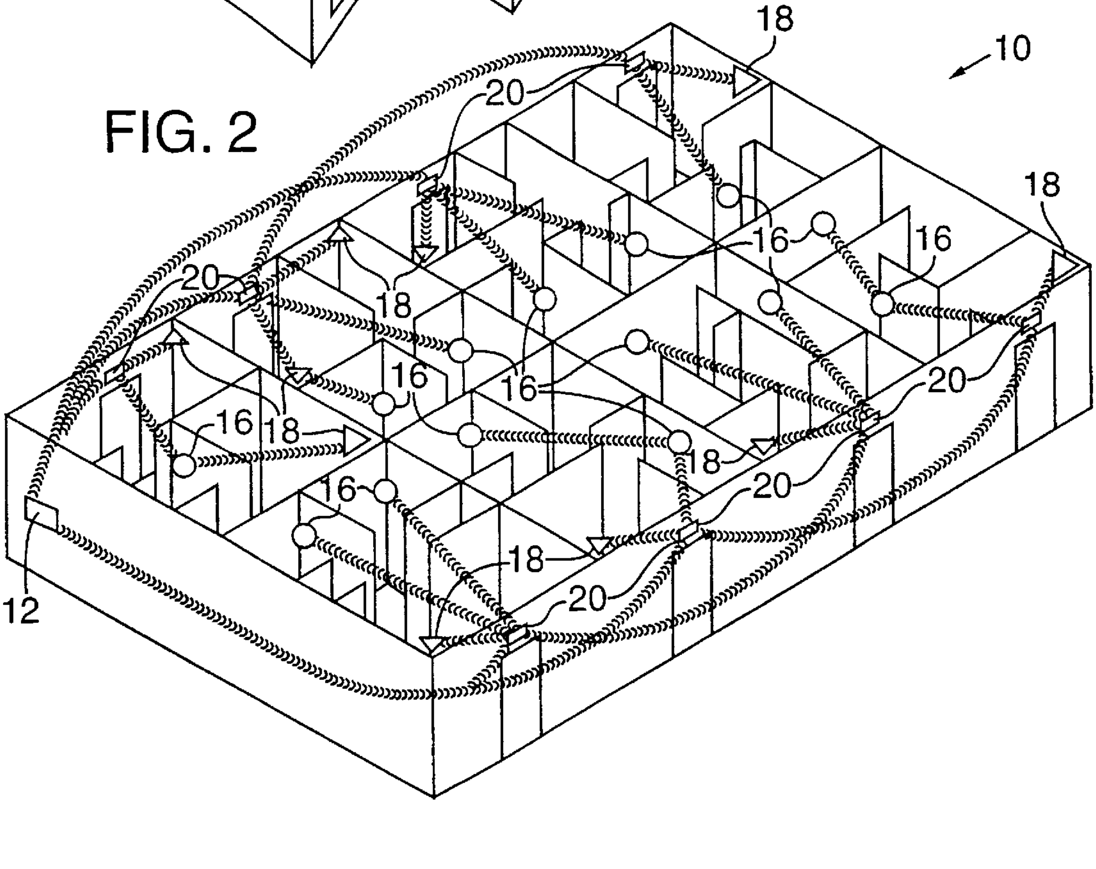

18
16
10
12
12
14
22
16
18
16
20
16
16

FIG. 2


18
10
20
18
16
16
20
18
16
16
20
16
18
18
20
16
12
18
20

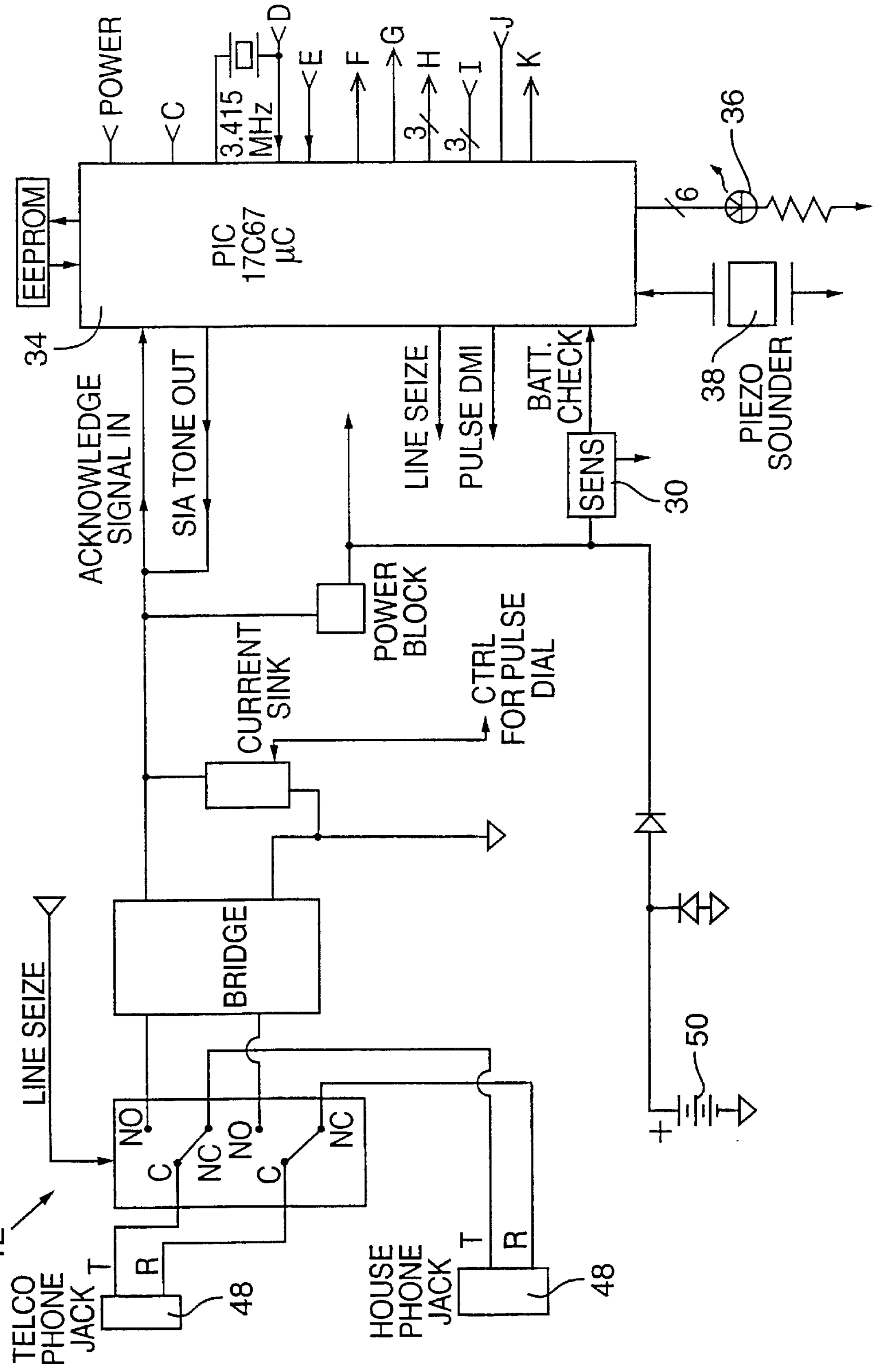

POWER
C
3.415 MHz
D
E
F
G
H
I
J
K
3
3
6
36
EEPROM
PIC 17C67 μC
34
ACKNOWLEDGE SIGNAL IN
SIA TONE OUT
LINE SEIZE
PULSE DMI
BATT. CHECK
SENS
30
38
PIEZO SOUNDER
POWER BLOCK
CURRENT SINK
CTRL FOR PULSE DIAL
BRIDGE
LINE SEIZE
NO
C
NC
NO
C
NC
12
TELCO PHONE JACK
T
R
48
HOUSE PHONE JACK
T
R
48
50
+

FIG. 3A

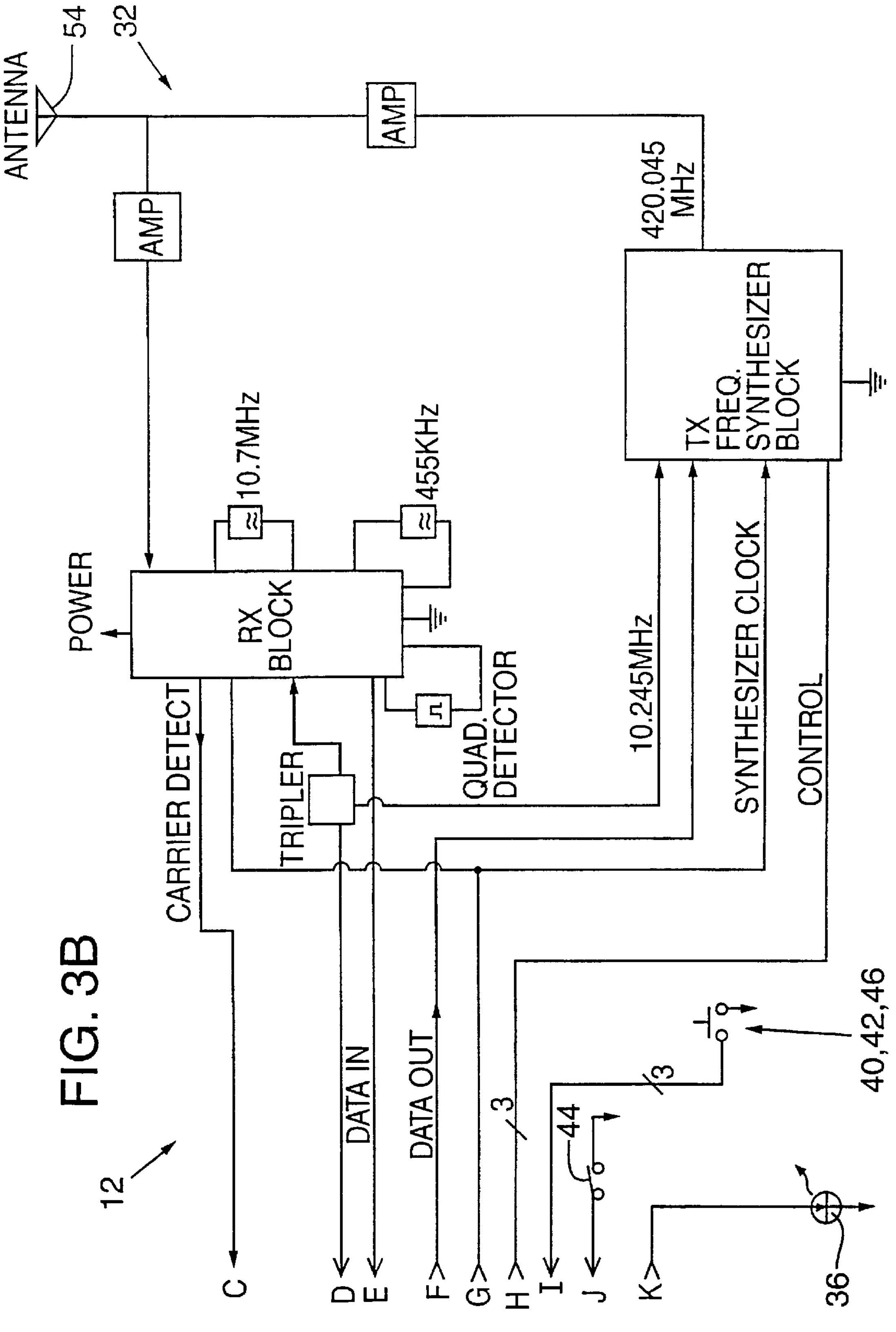

ANTENNA
54
32
AMP
AMP
420.045 MHz
TX FREQ. SYNTHESIZER BLOCK
POWER
RX BLOCK
10.7MHz
455KHz
QUAD. DETECTOR
TRIPLER
CARRIER DETECT
10.245MHz
SYNTHESIZER CLOCK
CONTROL
DATA IN
DATA OUT
3
3
44
40,42,46
36
12
C
D
E
F
G
H
I
J
K

FIG. 3B

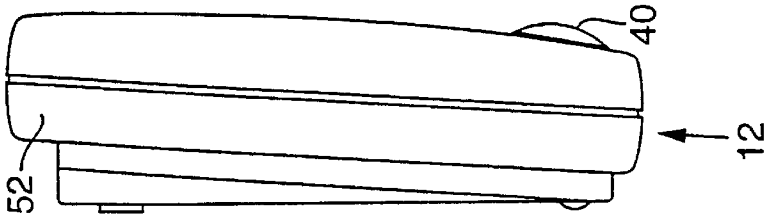


FIG. 4A

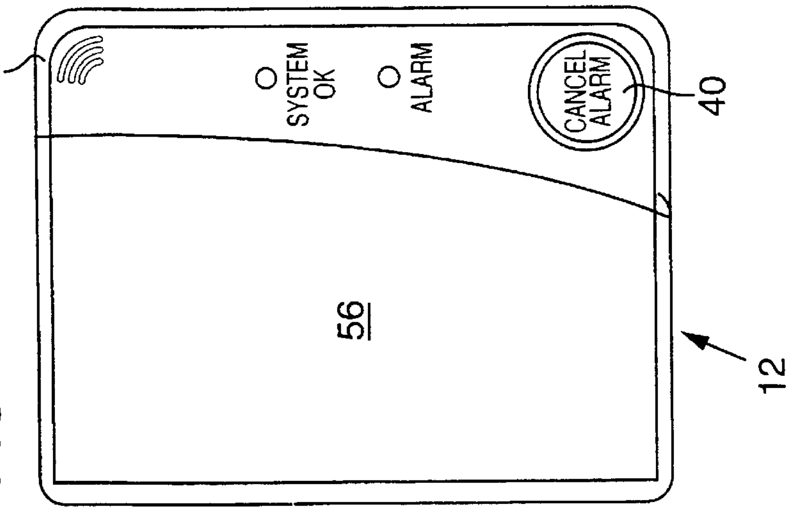

52
SYSTEM OK
ALARM
CANCEL ALARM
40
56
12

FIG. 4B

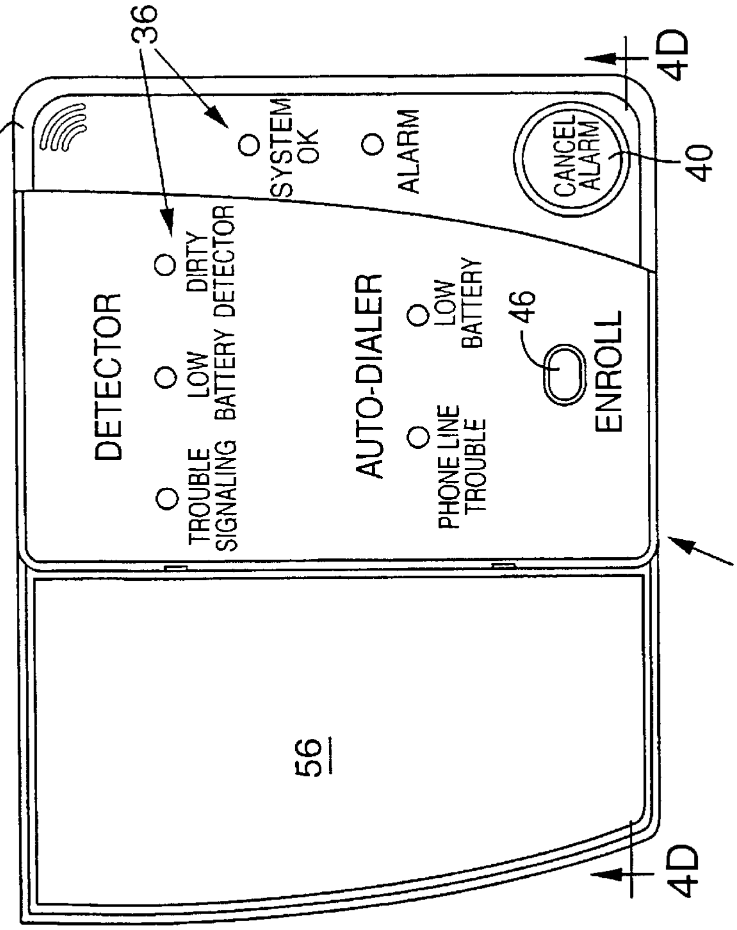

36
52
SYSTEM OK
ALARM
CANCEL ALARM
40
4D
DETECTOR
TROUBLE SIGNALING
LOW BATTERY
DIRTY DETECTOR
AUTO-DIALER
PHONE LINE TROUBLE
LOW BATTERY
46
ENROLL
12
56
4D

FIG. 4C

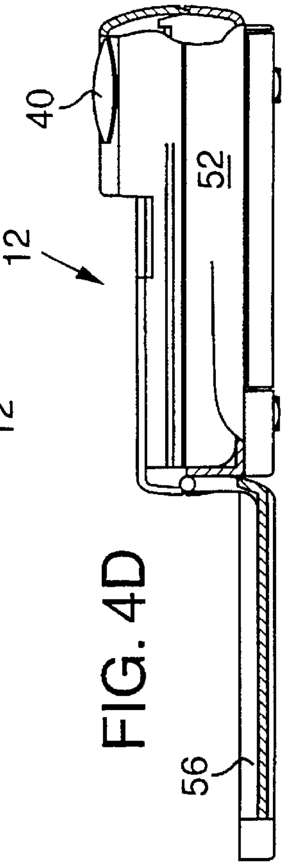


FIG. 4D

FIG. 5A

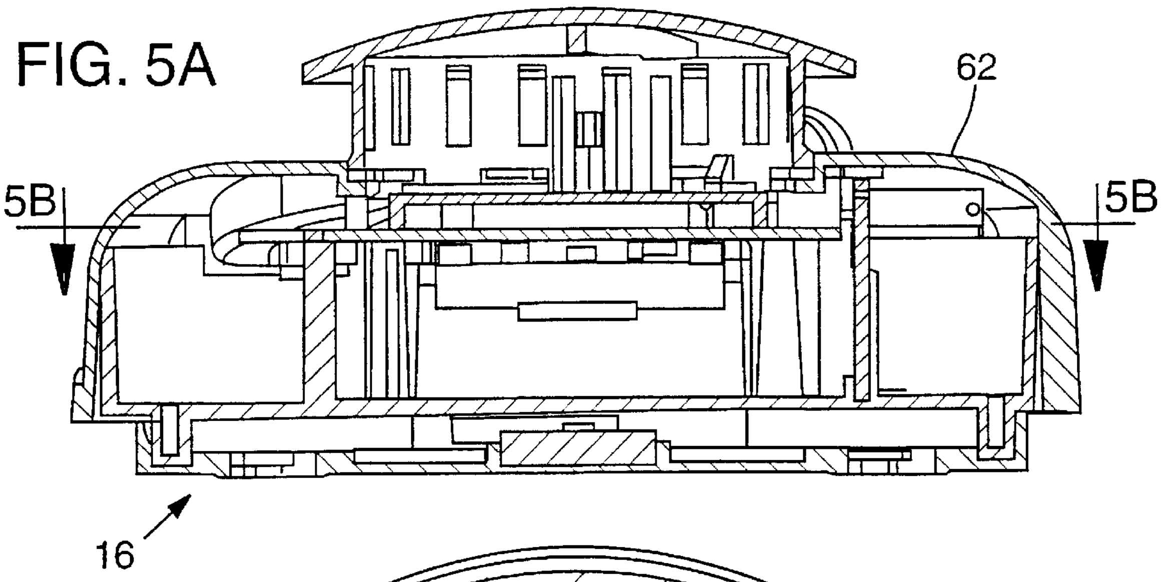
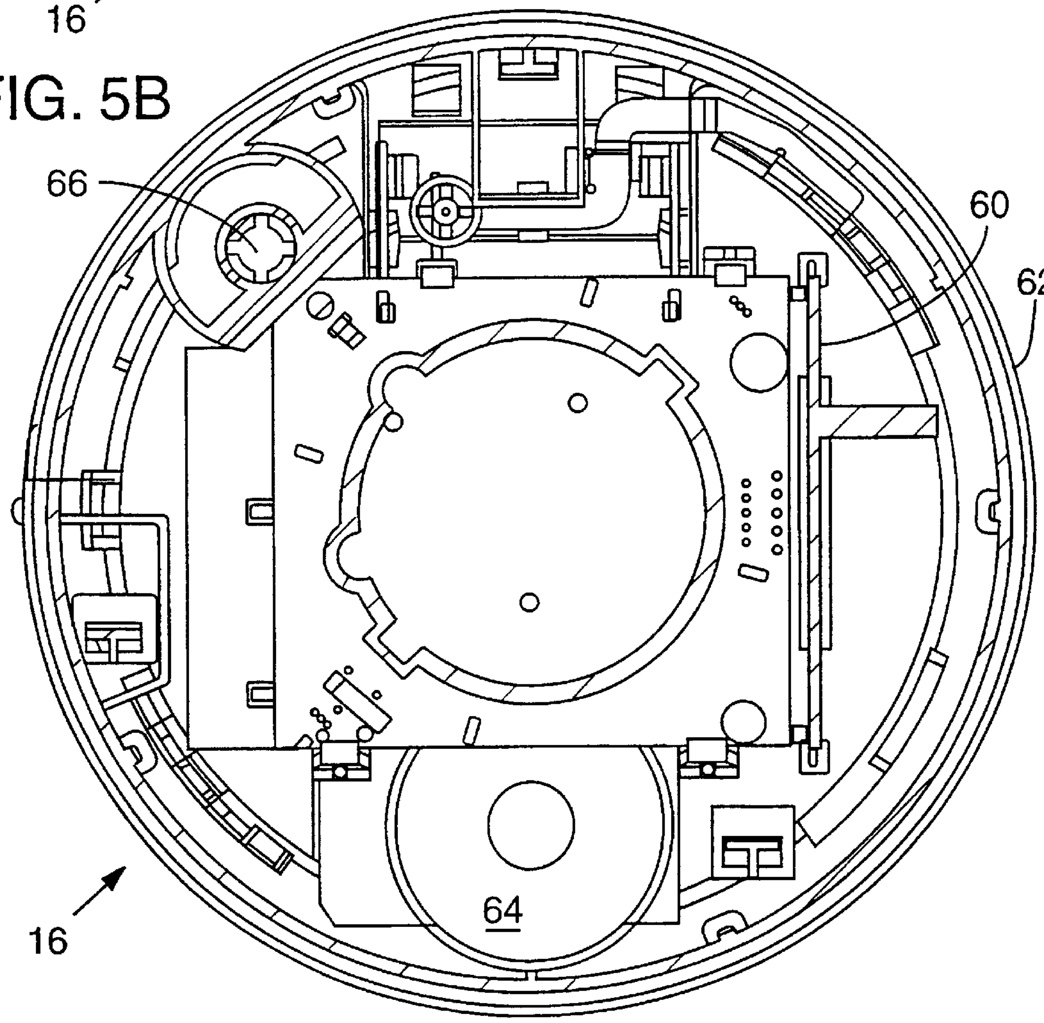


FIG. 5B


66
60
62
64
16

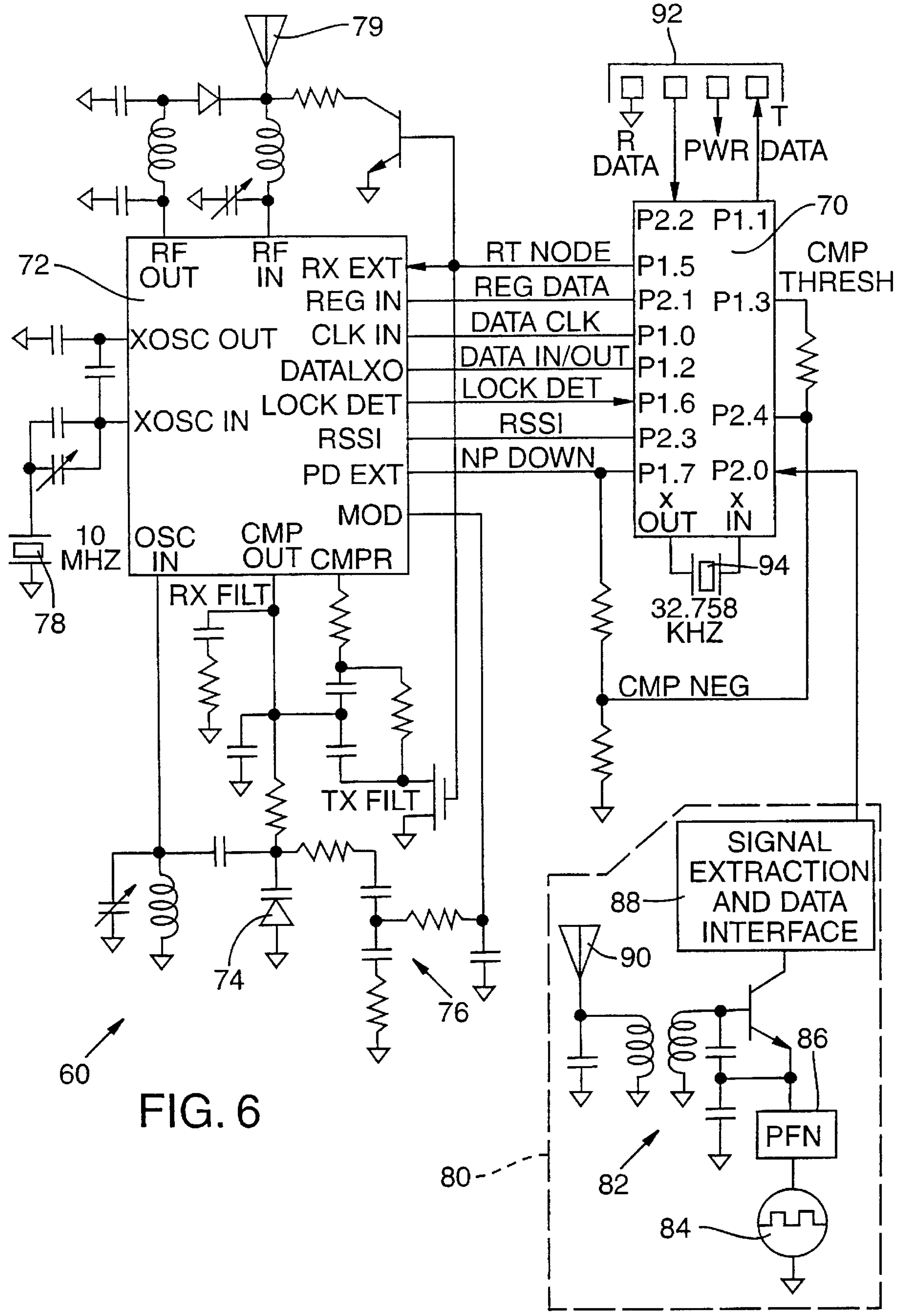

79
92
R DATA
PWR
T DATA
70
P2.2
P1.1
CMP THRESH
RT NODE
P1.5
72
RF OUT
RF IN
RX EXT
REG IN
REG DATA
P2.1
P1.3
XOSC OUT
CLK IN
DATA CLK
P1.0
DATALXO
DATA IN/OUT
P1.2
LOCK DET
LOCK DET
P1.6
P2.4
XOSC IN
RSSI
RSSI
P2.3
PD EXT
NP DOWN
P1.7
P2.0
MOD
X OUT
X IN
10 MHZ
OSC IN
CMP OUT
CMPR
94
78
RX FILT
32.758 KHZ
CMP NEG
TX FILT
SIGNAL EXTRACTION AND DATA INTERFACE
88
74
90
76
86
60
PFN
80
82
84

FIG. 6

WIRELESS HOME FIRE AND SECURITY ALARM SYSTEM

This application claims the benefit of Provisional application No. 60/103,432, filed Oct. 6, 1998.

TECHNICAL FIELD

This invention relates to fire and security alarm systems and more particularly to a wireless residential fire and security alarm system.

BACKGROUND OF THE INVENTION

Currently available wireless home fire and security alarm systems are usually part of a so-called wireless security system that requires a hardwired keypad, a base station, a hardwired siren, AC power connections, and an autodialer connection to a telephone line if the system is to be monitored. Such wireless systems actually require, therefore, considerable wiring, which makes them expensive to install and requires skilled installers.

In an effort to reduce costs and wiring, some prior workers have combined the keypad and the control panel into a single unit. However, this combination is bulky and inconvenient for wall mounting, which is required for keypad access but which renders difficult the installation of AC power, telephone, and siren wiring.

Other prior workers, in an effort to reduce manufacturing and installation costs, have further combined the siren into the keypad and the base station. However, few professional alarm installation companies will use such equipment because its security is compromised. For example, an intruder, upon hearing the siren, could simply smash the siren/keypad/base station or forcibly remove it from the wall and the alarm system and telephone autodialer dialer would be disabled. Therefore at least the autodialer needs to be separate from the keypad or siren to maintain adequate security.

Smoke detectors are key sensors in a fire alarm system. In prior wireless alarm systems, the smoke detectors are battery operated and include a small transmitter that transmits a fire alarm message to the control panel. To sound the alarm throughout the house, the control panel triggers a siren. In the frequently occurring event of a false alarm, the homeowner must use the keypad to reset the alarm and go to the location of the detector that caused the false alarm to reset the detector or place it into a "hush" mode.

Prior wireless sensors, such as intrusion sensors, transmit an alarm whenever they are tripped irrespective of whether the alarm system is armed. In kitchens and high traffic areas, such alarm transmissions can unnecessarily reduce the sensor battery life and can create signal contention problems when more than one sensor transmits at the same time. Reducing these unneeded transmissions would, therefore, be beneficial.

When the alarm system is armed and an actual alarm condition is detected, prior systems sound the alarm throughout the house with one or more sirens. Each siren requires a separate installation and is usually wired in, even in so-called wireless systems.

Because of the above-described limitation, prior wireless alarm systems are unduly complicated, especially for a typical homeowner to install or service, and do not have the benefits of typical hardwired systems. Accordingly, the full market potential of wireless home fire and security alarm systems has not been realized.

There are various U.S. patents that are potentially relevant to aspects of this invention. U.S. Pat. No. 4,363,031 for WIRELESS ALARM SYSTEM is described in the detailed description section of this application.

U.S. Pat. No. 5,686,885 describes sending a test signal along with an alarm signal from a smoke detector to differentiate a test event from an alarm condition.

U.S. Pat. No. 4,855,713 describes automatically "learning" the pre-assigned addresses in transmitters used for security systems.

U.S. Pat. No. 5,465,081 describes a wireless communication system that uses transceivers to communicate from one device to another in a loop configuration while modifying the message being sent around the loop to reduce the number of transmissions required during a supervision poll.

U.S. Pat. No. 5,486,812 describes a centralized locking system in which wireless transceivers are located in window and door locks to allow locking all doors and windows by a single transceiver based key fob button depression. If a door or window is open, the key fob is informed that complete locking cannot take place. This patent, like U.S. Pat. No. 5,465,081, describes a system in which messages are passed around a loop from one device to the next.

SUMMARY OF THE INVENTION

It is an object of this invention, therefore, to provide a low-cost, low-power, user installable, supervised alarm system that requires little or no wiring.

A wireless fire and security alarm system of this invention employs two-way transceivers in the smoke detectors, other sensors, and base station. The conventional keypad can be eliminated completely because the fire alarm system is reset by pressing a Test/Silence button built into every smoke detector or fire sensor and the security system is armed and disarmed by use of a wireless key fob sized transceiver. The separate siren is also eliminated because the siren in every smoke detector sounds an alarm throughout the building when any one of the smoke detectors detects a fire. This can be accomplished because every detector has a built-in transceiver and can, therefore, receive alarm messages from any other smoke alarm.

The AC power connection is also eliminated because the control unit is battery powered. Only a telephone wire connection is, therefore, needed for the system to be monitored. Moreover, in simple residential applications, the base station is not even needed unless centralized monitoring is required.

In multi-dwelling facilities such as apartments or college dormitories, smoke detectors in one dwelling space relay alarm conditions from dwelling space to dwelling space until reaching a centralized base station for the entire facility. This centralized base station can be located in facility manager's office for immediate notification of an alarm, improper smoke detector operation, low or missing battery indications, and dirty smoke detector indications. Such a wireless alarm system can save many lives in apartments, where smoke detectors batteries are often depleted or removed.

Another embodiment incorporates a long range wireless base station that communicates over standard cellular, GSM, or PCS type networks so that not even a telephone line connection is needed.

Further enhancements include battery conserving communications protocols, a simpler means of identifying and locating trouble conditions, an alarm verification mode for false alarms reduction, simple sensor enrolling and removing methods, and voice annunciation of fire location.

Primary features and operating modes of this invention are described below.

Automatic device addressing (enrolling) eases the addition and removal of smoke detectors, intrusion sensors, or other devices (collectively "sensors") from the alarm system. Programming is automatic, meaning that no address switches need to be set. No addresses need to be preprogrammed into device, and no address numbers need to be entered into the base station.

Enrollment is carried out by pressing an "Enroll" button on the base station, causing it to listen for new sensors. Inserting batteries into new sensors to be enrolled on the system causes the new sensor to send out a "new device" message. At this point, the sensor has no address, which marks it as a new device or one that has a previously defined "new device" message. Sensors, therefore, do not need to be uniquely preaddressed and can be generic from manufacturing. When the base station is in enroll mode and receives a new device message, the base station automatically enrolls the associated sensor into the system by downloading a house code address and a unit address to the new sensor. After the sensor is enrolled into the system, the sensor indicates enrollment by beeping its sounder, flashing its light-emitting diode ("LED"), or otherwise indicating that enrollment has been accepted.

Because sensors might lose their assigned addresses when batteries become depleted and require replacement, the following procedure eliminates confusion and automates the process. Pressing the "Enroll" button on the base station causes the base station to poll all the sensors in the system to determine which of the sensors are currently enrolled and how they are currently programmed. Then, removing the batteries from one sensor at a time, and inserting new batteries into that "new" sensor causes it to send the new device message because it has lost its addressing. When the base station receives the new device message, the base station initiates another poll of all sensors in the system. If one address is now missing, the base station assumes that the missing address is associated with the same sensor that is sending the new device message and then reloads the original address into the "new" sensor. As before, the sensor either beeps or flashes to indicate enrollment.

There are instances when devices must be removed from the system, such as when a sensor fails. If the failed sensor is not un-enrolled, the system recognizes that the failed sensor is missing and generates a continuing "RF Link" trouble message, until the failed sensor is repaired and returned to the system. When the Enroll mode is entered, the base station polls the system to determine which sensors are currently enrolled. Any nonresponding sensors are automatically removed from the current system status and are, therefore, no longer polled for supervision purposes and are unable to activate the system. In some cases, such as with security devices, to prevent unwanted tampering, entry of a security code may be required before a device can be removed from the system.

It is desirable to be able to reset a fire alarm system from any detector because false alarms are all too common. For example, cooking fumes, bathroom steam, or fireplace smoke can set off a smoke detector. In such cases, the homeowner would want to reset or silence the system as quickly as possible. U.S. Pat. No. 4,363,031 (the "031 patent") describes an unsupervised system that can reset a wireless fire alarm system from any sensor. However, the system requires two buttons, one for test and one for reset.

An improved and supervised one-button process of this invention provides each sensor with a "Test/Silence" button. If the system is in its normal non-alarm state when this button is depressed, the sensor sends a "Test" signal that signals all the sensor sounders to sound for a predetermined time and signals the base station to dial a test message to the monitoring station (if the test messages in the system are to be monitored). If the system is in an alarm condition or a test alarm condition, then pressing the Test/Silence button causes a "Silence" signal to be sent to the other sensors and the base station to silence the sounders and reset the alarm system. If the Test/Silence button is depressed during an alarm condition but before a preprogrammed autodialer delay (usually about 15 seconds), the base station is prevented from autodialing an alarm condition to the monitoring station.

Problem identification is another important consideration. In prior wireless alarm systems, a sensor having a low battery chirps its sounder and sends a trouble signal to the base station, which displays a low-battery trouble signal along with the address number of the affected sensor. Some sensors may also indicate a "dirty sensor" or an "out of sensitivity range" condition. As before, these sensors can chirp their sounders or flash LEDs, and send a message to the base station. If the sensor fails to properly communicate with the base station, in a supervised system the base station indicates a trouble condition and the address number of the affected unit. In an unsupervised system, a failure to communicate may not be detected by the system and will not, therefore, be reported.

The wireless alarm system of this invention overcomes these limitations because every sensor has a receiver and the system is supervised. When a low battery is detected by a sensor, instead of beeping, which is irritating when it occurs at night, a signal is sent to the base station, which sounds a quieter trouble sounder. Information regarding the nature of the trouble signal is retrieved by depressing a Diagnostic Mode button. A "Low Battery Detector" LED illuminates and the base station transmits a message to the appropriate sensor to sound for a predetermined time, preferably about three minutes, to identify which sensor requires fresh batteries.

U.S. Pat. No. 5,686,896 describes sending a pre-low battery report from a sensor to a central station and using a timer to delay triggering a local "low battery" alarm. The present invention, however, uses two different low battery thresholds and does not employ a preset time delay between the two different messages. Low battery signals may be sent to the base station for annunciation there rather than at the smoke detector, where it would be annoying. Locating the base station in a building manager's office or at a remote monitoring station also prevents the annoying local low battery alarm that sometimes causes renters and home owners to remove batteries. The second threshold detects when the battery is at the very end of its life and sounds the local alarm only when the battery is nearly depleted.

If the problem is a dirty detector sensor, the base station illuminates a "Detector Dirty" LED and transmits a signal to the affected sensor to sound.

If an alarm has occurred and the homeowner or the fire department needs to know which sensor originated the alarm, the same process can be used. When the base station is placed in Diagnostic Mode, a red "Alarm" LED flashes to indicate an alarm condition and sends a signal to the affected sensor to sound its sounder.

When a sensor ceases communicating with the system, it is difficult, if not impossible, to send the affected sensor a message to sound its sounder. Because the affected sensor has a transceiver, however, it can recognize that it has not been polled for a predetermined time and is unable to communicate with the system. The sensor responds by changing the flashing of its LED to a trouble pattern. This way, when the base station performs its normal hourly poll and discovers that a sensor is not responding, it illuminates an "RF Link" trouble LED alerting the homeowner to inspect each of the sensors to determine which one has its LED blinking the trouble pattern.

The alarm system of this invention provides a homeowner an ability to quickly identify and manage problems. However, the system can also be programmed so that all system trouble messages are monitored by a remote monitoring station, in which case trouble signals will be sent via the dialer rather than displayed locally.

The Consumer Product Safety Commission and the National Fire Protection Association report that approximately 30 percent of all residential smoke detectors are not operational because their batteries are dead, have not been replaced, or have been removed. To avoid this problem, supervised alarm systems monitor the operational status of sensors. However, batteries are removed mainly because of frequently occurring nuisance alarms. The above-described ability to silence the system from any detector reduces this problem. However, in a monitored system that can automatically summon fire or police services, reducing the number of false alarms is vitally important.

A false alarm reduction method commonly used in hardwired systems is referred to as alarm verification. Alarm verification has not been previously employed in wireless systems because they did not include receivers in each sensor. While the above-mentioned '031 patent describes a system capable of including a receiver in each smoke detector, it describes neither alarm verification nor system supervision capabilities. However, the alarm system of this invention provides the following alarm verification capability. When a sensor first generates an alarm signal, it sends an alarm message to the base station. If the base station is set to verify the alarm, it returns a reset message to the sensor. The base station starts a timer, and if that sensor or any other sensor in the system sends another alarm message within 60 seconds, the base station transmits a message to all sensors to sound their sounders.

There are significant benefits from having a fire alarm system in which all sensors sound when any one sensor detects an alarm condition. This feature, referred to as tandem operation, can provide up to four times more warning time in response to a fire alarm. For example, if a fire starts in a basement, a person asleep in a bedroom might not be alerted by his or her bedroom sensor sounder until it is too late to escape. For this reason, virtually all new construction codes since 1989 have required wired interconnected smoke alarm systems. Yet the vast majority of homes built prior to 1989 do not have such systems because of the wiring expense.

Prior wireless fire alarm systems that incorporate only transmitters in their sensors cannot receive messages to sound their sounders in the case of an alarm. Therefore an external siren is needed to sound a fire alarm throughout the house. The '031 patent describes a smoke detector system that includes receivers, but its protocol does not supervise each sensor. This omission prevents detection of any sensor that loses communication with the system. Accordingly, unsupervised systems are considered unreliable for use in security systems, and are even less reliable for use in fire alarm systems. Therefore, a supervised system is desirable.

This invention includes a two-way wireless alarm system in which the sensor is addressable and, therefore, can be supervised and have its sounder commanded to sound. The two-way wireless system of this invention communicates either directly to the base station or by passing messages through other sensors to the base station.

A person awakened by a fire alarm is often in a state of confusion, which can cause deadly evacuation delays. Therefore, vocal annunciation of the fire detection location is employed to evoke an efficient and appropriate response. This invention includes a smoke detector with a speaker that plays prerecorded vocal messages on command. Switches set by the homeowner during installation select an appropriate message, such as identifying on which floor the detector is being installed. Accordingly, when a fire is detected by a smoke detector installed on the first floor, the smoke detector can transmit a message to all the other smoke detectors to repeat a prerecorded vocal message such as, "Fire on First Floor."

Another advantage of this invention is that apartment or dormitory systems do not need a base station in each residence. Because each sensor includes a transceiver, a base station is required only if the system requires centralized monitoring, in which case a single base station provides the autodialer or other communication means, such as a cellular radio link. In apartments or dormitories, where living areas are close together, the two-way wireless system communicates from one living area to the next. One of the sensors is designated as a master sensor that acts as a communications hub for other sensors in that residence. The master sensor includes control functions and supervision functions, but not necessarily the autodialer or other communication means. Alarm and polling messages are transmitted from the master sensor of one residence to the master sensor in another residence, on to the next residence, and finally onto a base station, which is preferably installed in a manager's office. The base station provides the autodialer and other communications means, if monitoring is desired, or simply provides local monitoring.

This system supervises the operation of each sensor to ensure the sensors are properly powered, communicating, and not dirty. In one operational mode, a fire detected in a hallway can sound the sounders in the sensors in each residence on that floor. This alarm system provides superior monitoring and supervision of apartment and dormitory sensors and is considerably less expensive than prior systems because as few as one base station is required for an entire complex rather than one base station for each residence.

Some prior systems have tried combining the base station with the keypad, an arrangement that requires placing the keypad/base station in a central location close to telephone lines. However, the alarm system of this invention employs a supervised two-way wireless network that eliminates the need for hardwired sirens and a separate keypad. This invention allows resetting the fire alarm system from any sensor and, therefore, allows locating the base station close to existing telephone lines. Access to the base station is required only to review trouble conditions, as they arise. However, because the system can be monitored, it is possible for the monitoring center to manage these trouble problems, thus eliminating the need to display trouble conditions in the residence at all.

One embodiment of this invention employs a receiver that is enabled very briefly (one to two milliseconds every second) to reduce receiver electric current draw, thereby providing a battery life of many years. In an alternative embodiment, an ultra-low power "wake-up" receiver may be employed in each device to enable an asynchronous transceiver network that simplifies communications protocols and further reduces battery power requirements. Both embodiments eliminate the need for AC power wiring and the associated power supplies. The elimination of these extra wires simplifies and speeds installation, thereby enabling homeowners and relatively unskilled installers to install the systems. Improved fire protection is, therefore, practical in all homes including those built before 1989.

Another advantage of this invention is that all sensors sound an alarm even if a base station is damaged or non-operational. Possible causes include accidental damage, batteries depleted or removed, or wireless communications interference or blockage. In such instances, it is desirable for all sensors to sound an alarm if a fire is detected. This is possible in the alarm system of this invention because each sensor is able to confirm whether its alarm message has been received by the base station. If after repeated attempts, the base station fails to respond, the sensor automatically transmits its alarm message to the other sensors, which sound their sounders.

When prior panic buttons were pressed, the user could not be certain whether the panic message was received by the monitoring station. However, this invention may also include an emergency response button having an audible confirmation. This is possible because this invention can readily include a combination of sensor types each including built-in transceivers selected from among smoke detectors, security sensors, wireless two-way keypads, hand-held wireless key fobs, energy management devices, thermostats, meter readers, and wireless emergency panic buttons. However, the panic button of this invention includes a transceiver and a mini-sounder that beeps in response to an acknowledgment message received from the monitoring, station by way of the base station.

Additional objects and advantages of this invention will be apparent from the following detailed description of preferred embodiments thereof which proceed with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a simplified isometric pictorial view of an exemplary wireless fire and security system of this invention installed in a residence.

FIG. **2** is a simplified isometric pictorial view of an exemplary wireless fire and security system of this invention installed in an apartment building.

FIGS. **3**A and **3**B are a simplified electrical block diagram of a wireless base station of this invention.

FIGS. **4**A, **4**B, **4**C, and **4**D are respective side, front (with door closed), front (with door open), and bottom cross-sectional views of a case housing the base station of FIGS. **3**A and **3**B.

FIGS. **5**A and **5**B are respective sectional side and top pictorial views of a wireless smoke detector of this invention showing a preferred transceiver board mounting location.

FIG. **6** is a simplified schematic electrical circuit diagram of a preferred transceiver employed in sensors, base stations, autodialers, and other devices used in the wireless fire and security systems of this invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIGS. **1** and **2** show respective home and apartment configurations of a wireless alarm system **10** including a base station **12**, a keypad **14**, smoke detectors **16**, passive infrared ("PIR") motion detectors **18**, door/window contacts with sounders **20**, and a glassbreak detector **22** (collectively "sensors"). Wireless alarm system **10** may further include phone jack line seizure modules, wireless voice evacuation smoke detectors, sounders, carbon monoxide detectors, heat detectors, combination smoke and heat detectors, and personal emergency pendants.

Referring to FIGS. **3** and **4**, base station **12** includes a battery level sensor **30**, a transceiver **32**, a microprocessor **34** implementing a digital autodialer, seven diagnostic LEDs **36**, a sounder **38**, a large "cancel/silence" button **40**, a diagnostic test button **42** (activated by opening a base station **12** door), an alarm verification switch **44**, an "enroll" button **46**, and two telephone connectors **48**. Wireless alarm system **10** is powered by a battery **50** and employs telephone current when dialing. Battery **50** preferably comprises three user-replaceable AA batteries that are accessible in power base station **12**.

Base station **12** is enclosed in a case **52** made of textured white ABS plastic including provisions for private labeling. Case **52** is slightly larger than the size of a double gang wall plate and is about 3.81 cm (1.5 in. deep). Case **52** may be wall mounted, such as over a recessed telephone jack, and includes two telephone connectors **48**, one for a telephone and the other for a telephone line. Transceiver **32** is coupled to an antenna **54**, both of which are housed inside case **52**. Each of keypad **14**, smoke detectors **16**, PIR motion detectors **18**, door/window contacts with sounders **20**, and glassbreak detector **22** includes a transceiver, such as transceiver **32**.

Case **52** includes a door **56** that conceals LEDs **36**, enroll button **46**, and an operating instruction label (not shown). Opening door **56** activates a diagnostic test mode of base station **12**.

A battery powered base station **12** is highly desirable because it reduces costs, does not require AC power wiring and power supplies, and is easier to install. To accomplish this, base station **12** activates transceiver **32** periodically to detect incoming messages and then deactivates transceiver **32** when no messages are detected. Because security systems require rapid response, transceiver **32** activations occur at least about once per second. The receiving time period and transceiver **32** current draw are relevant parameters for reducing the resulting power consumption to a point where battery operation is practical.

Crystal controlled single frequency receivers can activate and stabilize fairly rapidly (less than 2 milliseconds) and require fairly low operating currents (less than 20 milliamps). This does not, however, enable multiple frequency reception, which is useful for avoiding environmental interference or frequency band crowding.

Frequency synthesized receivers can change operating frequencies under microprocessor control. However, such receivers require time to determine the proper frequency, load the frequency registers, and stabilize a phase-locked loop before the receiver is actually activated. Accordingly, a typical synthesized receiver can take over 4 milliseconds to load its registers and another 0.6 to 2 milliseconds to stabilize the phase-locked loop. This does not meet the requirements for battery operation.

Therefore, transceiver **32** of this invention preloads the frequency registers and stores the frequency in those registers even when the receiver is deactivated, thereby requiring only 0.6 to 2 milliseconds to detect incoming signals. Transmit frequency registers are similarly employed to conserve battery life during transmissions.

Another requirement affecting battery powered operation is the time required to successfully decode a message once it is received. In conventional systems, alarm transmissions, even if repeated eight times, take less than 0.1 second to complete. Some messages might take longer, but most alarm messages are quite short. The sensor address information consumes most of the message length. However, if the receiver is activated for only 1–2 milliseconds per second, the chances are poor of detecting a typical message.

Detecting a typical message is accomplished by transmitting a message that lasts at least as long as the time period the receiver is deactivated. The message can repeat continuously during that time period, or a preamble to the message can be transmitted during the time period. The preamble informs the receiver of an incoming message and keeps the receiver activated to receive the message at the end of the preamble. After the receiver has received the message, the receiving device communicates back to the originating device without a preamble because the originating device is already activated and awaiting a response. Therefore, once the necessary devices are activated by the first transmission, then a series of messages can be exchanged without the use of preambles. After the messages are completed and no further incoming messages are detected, the receivers return to their periodic activation cycles.

The Federal Communications Commission ("FCC") has established regulations governing alarm transmission periods, power levels, and unlicensed transmission bands. Because the regulations limit transmission time to one second, the receiver activation, detection, and deactivation period is less than a one second.

Cancel/silence button **40** is exposed on base station **12** to serve two functions. During a fire alarm condition, depressing cancel/silence button **40** resets all smoke detectors **16** and sends a restore signal to a central monitoring station. During a trouble condition, depressing cancel/silence button **40** temporarily silences sounder **38** in base station **12**.

The seven diagnostic LEDs **36** annunciate the following conditions: Yellow trouble LEDs indicate "Dirty Detector," "Sensor Low Battery," "Base Low Battery," "Radio Link Trouble," and "Phone Line Trouble;" a red LED indicates "Alarm/Dialing;" and a green LED indicates "System OK."

Base station **12** enters diagnostic mode when door **56** is opened. Diagnostic mode energizes particular ones of diagnostic LE s **36** corresponding to troubles detected in alarm system **10**. Base station **12** exits diagnostic mode after 10 seconds and returns to its normal operating state.

Alarm verification switch **44** is a two-position switch that is located in the battery compartment of base station **12**. An "on" position activates the fire alarm verification feature, which causes base station **12** to transmit a "restore/reset" message to an initiating one of smoke detectors **16** when an initial "fire alarm" message is received. Then, if a second or subsequent fire alarm message is received from any of smoke detectors **16** within 60 seconds, base station **12** activates a fire alarm by sending a "sounder on" message to smoke detectors **16**. Base station **12** waits an additional 15 seconds before dialing the central monitoring station.

Sounder **38** in base station **12** "chirps" to draw attention to trouble conditions present anywhere in alarm system **10**. A short chirp interval minimizes current draw from battery **50**. Chirping sounder **38** eliminates the need to chirp sounders in any of smoke detectors **16** and thereby eliminates a nighttime nuisance. Sounder **38** can be silenced by pressing cancel/silence button **40** on base station **12**.

The digital autodialer implemented by microprocessor **34** dials a user programmable telephone number. During a predetermined event, the programmable telephone number is dialed and pertinent information is communicated to the central monitoring station. Preferred predetermined events include "fire alarm," fire restore," "battery low," and "test." During these predetermined events, the autodialer seizes the telephone line and communicates via the SIA-DCS protocol. The autodialer preferably stores a primary telephone number and a back-up telephone number. Base station **12** first attempts to dial the primary phone number, and after three failed attempts, it makes three attempts to dial the back-up phone number. If all attempts fail, a phone line trouble condition is indicated on one of LEDs **36**.

Base station **12** of this invention will remain fully functional for at least 30 days and sounder **38** will operate for at least 10 days after a low battery condition is detected. Battery **50** has an operating life of about two to three years and reaches a low condition when it is depleted to approximately 2.7 volts.

FIGS. **5**A and **5**B show a typical one of wireless smoke detectors **16**, which are based on conventional smoke detectors with a transceiver **60** added inside a housing **62**. Smoke detectors **16** preferably operate on the photoelectric principle and contain options for fixed temperature heat sensing to meet the needs of the security fire alarm systems market. Of course ionization or other types of smoke detectors can be used as well.

Smoke detectors **16** are powered by 3 AA alkaline batteries (not shown), which also power transceiver **60**. Smoke detectors **16** are self-restoring devices with sounders **64** that are actuated when in an alarm mode. Sounders **64** may be silenced by depressing a "test/silence" button **66**. The smoke detector electronics employ a microcontroller based architecture that includes automatic sensitivity checks to verify whether the detector is within its specified sensitivity limits. Such sensitivity checking is described in U.S. Pat. No. 5,546,074 for SMOKE DETECTOR SYSTEM WITH SELF-DIAGNOSTIC CAPABILITIES AND REPLACEABLE SMOKE INTAKE CANOPY, which is assigned to the assignee of this application. If the sensitivity changes are caused by dust and dirt, the detector automatically compensates by adjusting its sensitivity accordingly. Such automatic compensating is described in U.S. Pat. No. 5,798,701 for SELF-ADJUSTING SMOKE DETECTOR WITH SELF-DIAGNOSTIC CAPABILITIES, which is assigned to the assignee of this application. The maximum daily adjustment is 0.1%/ft. every 24 hours, with a maximum deviation of 1.0%/ft. with respect to the original factory set sensitivity. When the maximum sensitivity is reached, it will not change with further accumulation of dust. When the sensitivity drifts outside the specified limits, it visually notifies the user by extinguishing a normally flashing red LED (not shown). Smoke detectors **16** also transmit trouble and test messages to base station **12**.

The photoelectric versions of smoke detectors **16** acquire ambient obscuration data every nine seconds. The red LED blinks every time a sample is taken. If any one sample is above the calibrated alarm threshold, two more samples are taken at about 4.5 second intervals. If all three samples are above the calibrated alarm threshold, the detector enters alarm condition until obscuration returns to normal, at which time the detector resets.

An optional photo/heat sensor continuously monitors ambient thermal conditions. An alarm condition is entered if the ambient temperature exceeds 57° C. independent of the rate of thermal change. A low temperature alert can also be sent when temperatures drop below 7° C., as an indication that heat has been lost in the home and potential freezing conditions are present.

As set forth in the above-described U.S. Pat. No. 5,798,701, the photoelectric detectors automatically adjust their sensitivity every 24 hours to compensate for dust build-up in the sensing chamber. The detectors adjust their sensitivity by averaging 4 samples taken every 30 minutes, and storing the minimum and maximum average taken over a 24 hour period. The closest minimum or maximum average to the clean air measurement stored during calibration is used to adjust the detectors sensitivity. The maximum adjustment allowed in a 24 hour period is 0.1%/ft. The total adjustment is limited to 1.0%/ft. for detectors becoming more sensitive, and 0.2%/ft. for detector becoming less sensitive.

When any of smoke detectors **16** enter alarm mode, the associated sounder **64** is activated. Sounders **64** in all smoke detectors **16** may be silenced by pushing "test/silence" button **66** on any of smoke detectors **16**.

Smoke detectors **16** display a trouble condition by extinguishing the red LED. A trouble condition exists when any one of smoke detectors **16** fails the auto test or falls out of the specified sensitivity limits for a 24 hour period. The process for determining whether a smoke detector is out of its sensitivity range is as follows: If an obscuration sample falls outside the sensitivity limits, a 24 hour time-out begins. If at any time within this 24 hour period the smoke detector has 3 consecutive samples within the sensitivity limits, the 24 hour timer is reset.

Another trouble condition exists when any one of smoke detectors **16** detects a low battery condition. The red LED is extinguished and a "low battery" message is sent to base station **12**, which begins chirping sounder **38** (FIG. **3A**). If base station **12** "cancel/silence" button **40** is pushed, then the smoke detector with the low battery condition starts a trouble chirp of its sounder **64** for three minutes and then resets. Sounder **64** can be silenced by pushing "test/silence" button **66** of the smoke detector during the three minute period. If base station **12** has failed and, therefore, does not respond, then the smoke detector enters a default mode and chirps its sounder **64** to indicate a low battery condition.

Optionally, any of the sensors and other battery operated devices, such as keypads and dialers, can employ two separate low battery thresholds. One low battery threshold is set for communicating "low battery" messages through the dialer to a remote monitoring station. This message is usually sent first. A second threshold is used to signal the low battery condition locally. This allows the remote monitoring station time to set up a service call before the local low battery signal begins to sound.

Each of smoke detectors **16** is desirably fully functional for at least 30 days after a low battery condition is detected. Sounders **64** have at least an 85 dB sound intensity at 10 ft. when sounding a temporal sounding pattern, and operate nominally for at least four minutes in the alarm mode after a low battery condition is detected. Battery life is at least two years.

Referring to FIGS. **1**, **4**, and **5**, alarm system **10** is easily end user programmable as follows:

Depressing "Enroll" button **46** on base station **12** places alarm system **10** in an enroll mode. Base station **12** selects, from among allowed frequencies, a random operating frequency, which becomes a special network frequency. Base station **12** broadcasts the system number on the special channel at full power. If another alarm system is within range and has the same system number, then base station **12** randomly selects another "special" frequency. Base station **12** reduces its transmit power level to half, to carry out enrollment, and stays awake for the entire enrollment process.

To enroll a sensor being added to alarm system **10**, batteries are installed in the added sensor, which causes it to transmit to base station **12** a device type code ("DTC") message including a sensor serial number.

Base station **12** recognizes that the DTC is associated with an added sensor and returns a "teaching" message that programs the added sensor with the system configuration and a unit address. The teaching message includes an assigned frequency for the sensor, the system number, a logical device address, and an echo of the sensor serial number. Additional information can be downloaded during or after enrollment.

The added sensor confirms acceptance of this programming by chirping its sounder once.

After all of the sensors are enrolled in the system, base station **12** automatically exits "Enroll" mode after ten minutes. The homeowner can then depress "test/silence" button **66** on any of smoke detectors **16** to test alarm system **10**. The smoke detector **16** initiating the system test sends a "test" message to base station **12**, which responds by sending a "sound temporal pattern" message to all sensors, which activate their sounders for two minutes. The autodialer implemented in base station **12** may also send a "test signal" to the phone number programmed into the dialer.

De-enrollment is initiated by:

A specific "de-enrollment" message.

If a device fails to respond to a "find sensor" message (normally issued if the sensor misses a supervision message), base station **12** retains the missing device-information in the configuration table for one day (in case of battery change), and reports the missing device information to the central monitoring station. After the one day period, if the sensor is still missing, base station **12** de-enrolls the device and its system number will be reused. The "find sensor" message is not transmitted to devices that have reported a "low battery level 2" condition.

When changing the battery in a previously enrolled device, the device resets itself and is re-enrolled into alarm system **10**. If the re-enrollment is within the one day period, base station **12** reassigns the original information to the re-enrolled device.

If base station **12** is inoperative, the sensors will sound, and the user attends to removing the batteries from all the sensors. If the batteries in base station **12** are changed in an orderly manner (this implies that the sensors receive a "base station down" message before missing a synchronization burst), the sensors will not sound, and alarm system **10** will respond normally after the batteries are replaced.

Referring also to FIG. **2**, the enrollment procedure for apartments and dormitories is carried out as follows:

Each living area is assigned its own "housecode" just like installations in a home (FIG. **1**). However, a "facility code" is added to the housecode to identify the apartment complex, or dormitory building. In most applications, the housecodes become a small number of digits, and the facility code becomes larger. Every sensor transmits both codes, and the receivers listen for both codes to be correct before decoding the data.

To enroll sensors in an apartment complex or dormitory building, base station **12** must first be installed. Base station **12** is manufactured with a preprogrammed pre-defined facility code. Then, when installing alarm system **10** in an apartment or dormitory room, a "hub device" for that living area must be installed first. FIG. **2** shows door/window contacts with sounders **20** being employed as the hub devices, but any device may be employed as a hub device. This is done by placing base station **12** in "enroll" mode and then inserting batteries into the selected hub device. The hub device has no pre-programmed facility or house codes and, therefore, sends a "new device" message to base station **12**. Upon receipt of this new device message, base station **12** downloads the facility code, and assigns an available housecode to that hub device. Each hub device, in each living area, is assigned a different housecode. Once the hub device has its assigned facility code and housecode, the remaining devices in that living area are enrolled as explained above for a home.

Frequency assignment during enrollment of added sensors is carried out as follows:

When an added sensor has batteries installed during the enrollment process, it transmits a "new device" message to base station **12**. Because base station **12** can operate on a number of available frequency channels, base station **12** may not receive the new device message if it is sent on the wrong channel. There are two possible solutions for resolving this problem. Either base station **12** automatically starts scanning all the available frequencies when placed in enroll mode until it recognizes an incoming new device message, or the added sensor transmits the new device message on the first channel, and if no answer is received within one second, the added sensor automatically transmits on the second channel. This is continued until the added sensor receives an answer back.

Once the added sensor and base station **12** link up on the same frequency, then base station **12** can download the proper operating channels and housecode, unit address, and other data to the added sensor and complete the enrollment process.

The same two-way wireless system can readily be used in commercial applications. Most of the functionality remains the same, and many of the security and fire sensors remain virtually unchanged. However, one difference is that commercial sites can cover much greater areas and distances. Therefore, data transmissions will more likely be sent through intermediary devices to reach the fringe units, and in some cases require multiple hops. The system architecture for such a large system would be very similar to the apartment or dormitory system of FIG. **2**. In this case the entire commercial site would have a facility code originally supplied in base station **12**. Then the system would automatically identify hub devices throughout the facility. This can be done by manufacturing some devices as unique hub devices and having them installed throughout the site, or preferably by incorporating a additional memory and processing power in each device to allow for automatic system configuration wherein any device can be assigned as a hub device.

Each hub device in the commercial system functions similarly to hub devices in the apartment or dormitory system of FIG. **2**. However, rather than having a housecode, they simply have a hub code.

The typical operational interaction of base station **12** and smoke detectors **16** of alarm system **10** is summarized below in Table 1.

TABLE 1

Event	Smoke Detector Action	Base station 12 Action
Fire alarm signal with alarm verification turned off	Initiating smoke detector goes into alarm and sends a signal to the base station 12 to alarm, base station 12 signals all other detectors to start their sounders. The initiating detector's red LED is latched on, all other smoke detectors LEDs are off.	If no cancel signal is received within 15 seconds, autodialer dials phone number to communicate an alarm. Before dialing, the "Alarm" LED flashes. When the dialer seizes the telephone line, the "Alarm" LED is on steady. The LED stays on until the Alarm condition is restored or the Cancel/Silence switch is pressed. Dialer reports base station 12 house/account code and fire alarm condition.
First fire alarm signal with alarm verification turned on	Initiating detector goes into alarm and sends a signal to the base station 12 to alarm. The base station 12 sends a reset signal to the initiating detector.	Dialer remains normal. Sends reset signal back to initiating detector
Second fire alarm signal from any detector within 60 seconds with alarm verification turned	Initiating detector goes into alarm and sends a signal to the base station 12 to alarm, the base station 12 signals all other detectors to start their sounders. The initiating detector's red LED is latched on, all other smoke detectors LEDs are off.	If no cancel signal is received for 15 seconds, communicator dials phone number to communicate an alarm. Before dialing the "Alarm" LED flashes and then goes solid until the Alarm condition is restored or the Cancel/Silence switch is pressed. Dialer reports base station 12 house/account code and fire alarm condition.

TABLE 1-continued

Event	Smoke Detector Action	Base station 12 Action
on Detector "Test/Cancel" button pushed during verification period or first 15 seconds of alarm	Pressed detector silences and sends silence/cancel signal to base station 12. All detectors reset after command from base station 12.	Base station 12 sends silence/cancel signal to all detectors. Base station 12 returns to normal operation
Base station 12 "Cancel/Silence" button pushed during verification period or first 15 seconds of alarm	All smoke detectors reset.	Base station 12 sends silence/cancel signal to all detectors. Base station 12 returns to normal operation.
Smoke detector button pushed after 15 second base station 12 delay	All detectors are silenced, and reset after receiving command from from base station 12.	Dialer communicates restore to central station. Base station 12 sends silence/cancel signal to detectors.
Initiating smoke detector clears alarm condition itself	Sends restore or cancel condition to base station 12. All detectors go silent if all detectors are clear of smoke. has been communicated.	If all units are clear, the base station 12 sends silence/cancel signal to all detectors. Sends restore signal to the central station if Alarm
Detector "test/cancel" button pushed during normal operation	Test signal sent to base station 12. Sounders on all detectors are energized. Sounders will automatically silence within 2 minutes. If test button is pushed again during the 2 minute period all sounders will silence. Any real fire alarm signal will override test conditions	Base station 12 sends test signal to all detectors. Base station 12 communicator dials phone number immediately without delay. Sends test signal to the central station.
Communication of test signal successful	N/A	Base station 12 resets to normal condition
Communication of test signal not successful	N/A two separate numbers.	Trouble sounder on base station 12 chirps after three failed communication attempts on
Opening compartment door after failure of communication's test	N/A	Trouble sounder silences. Phone Line Trouble LED is energized for 10 seconds, and then resets
Detector drifts out of UL sensitivity range	LED on detector is extinguished. CleanMe ® signal sent to base station 12	Trouble sounder chirps
Opening compartment door during CleanMe ® signal condition	Sounder in dirty detector chirps for 3 minutes and the LED blinks rapidly.	Trouble sounder silenced and "Dirty Detector" LED is energized for 10 seconds. Sounder will chirp again every 24 hours if dirty detector condition persists.

TABLE 1-continued

Event	Smoke Detector Action	Base station 12 Action
Low battery condition on a detector	LED on detector is extinguished. Low battery signal sent to base station 12.	Trouble sounder chirps.
Opening compartment door during low battery condition	Sounder in detector with low battery chirps for 3 minutes	Trouble sounder silenced and "Sensor Low Battery" LED energizes for 10 seconds. Sounder will chirp again every 24 hours if low battery condition persists.
Low battery condition on the base station 12 battery.	N/A	Trouble sounder chirps.
Opening compartment door during low battery condition on the base station 12 battery	N/A	"Base station 12 Low Battery" LED energized for 10 seconds and base station 12 sounder sounds steady for 10 seconds. Sounder will begin chirping again within 24 hours if low battery condition continues to exist
Base station 12 low battery falls to level just before inoperability.	N/A	Base station 12 dials central station to report base station 12 low battery.
Base station 12 "Cancel/ Silence" button pushed during telephone line trouble condition	N/A	Trouble sounder is silenced after the Cancel/Silence button is pressed. After opening the door, "Phone Line Trouble" LED is energized for 10 seconds.
Base station 12 fails to receive supervision signal from any detector for more than one hour.	N/A	Trouble sounder chirps.
Opening compartment door during system RF link trouble condition.	N/A	Trouble sounder is silenced, and "RF Link Trouble" LED is energized for 10 seconds and then extinguishes.
"Alarm Verification" switch "ON".	N/A	Alarm verification programming implemented in base station 12. Base station 12 will ship with this as default position.
"Alarm Verification" switch "OFF".	N/A	Alarm verification programing not implemented in base station 12.
"Enroll" button activated and batteries added to device. (This is the same process required for adding a new device or changing batteries on an	Detector begins to signal the base station 12.	When base station 12 receives signal from detector it will enroll it as the appropriate detector within the system, e.g. first signal received will be detector 1, second signal received will be detector 2 . . . etc. Base station 12 sends signal back to detector teaching the detector its identity.

TABLE 1-continued

Event	Smoke Detector Action	Base station 12 Action
existing device.)		
Signal sent back to the detector from the base station 12 when in "enroll" mode.	Detector accepts programing and chirps.	N/A
Opening compartment door during normal conditions.	N/A	Green "System OK" LED energized for 10 seconds and then extinguishes.
Base station 12 idle.	N/A	All LEDs off.
Base station 12 batteries completely dead or base station 12 not functional and Smoke Detector initiates an Alarm.	After failure to communicate, the Smoke Detector sends an alarm message directly to other smoke detectors to turn on their Sounders. Alarm verification process is overridden.	N/A

Referring to FIGS. **3** and **6**, alarm system **10** employs two-way wireless transceivers to avoid problems caused by deliberate or circumstantial jamming, range problems (especially in steel construction), multiple message contention, false alarms, reliability, message integrity, and power consumption. Transceivers **32** and **60** avoid jamming by automatically switching frequencies, when necessary, to an alternate channel within an FCC approved frequency band. Transceivers **32** and **60** check alarm system **10** status by periodically polling sensors and by validating and acknowledging received messages to eliminate false alarms. Transceivers **60** are configured to typically communicate directly with transceiver **32** in base station **12**. However, when remote transceivers **60** are outside the range of base station **12**, messages are automatically routed via any other in-range transceiver in alarm system **10**.

The transceiver-based alarm systems of this invention differ from conventional wireless systems because they are interactive multi-path loop systems rather than blind broadcasts, they are two-way message transporting systems rather than one way radio nets, they have intelligence at every transporting unit instead of only at a centralized base station, and they combine local intelligence with frequency synthesized base station **12** to circumvent interference by automatically switching frequency or finding alternate pathways for sending and receiving messages. These differences are described more fully below.

A conventional broadcast communication system transmits a signal on a predetermined frequency to receivers within a given "net" area or segment. Any receiver within the "net" or segment that is tuned to the same frequency will pick up the signal. The transmitter must be sufficiently powerful to reach the furthest sensor or control, which is a battery life limitation. Moreover, the greater the range from the transmitter the greater the chance of noise corruption and interference with other systems. The sensor receivers can be made more sensitive to improve range, but this increases the occurrences of noise corruption and interference. The transmitter signal propagates "line-of-sight," so obstructions may affect it. Therefore, a broadcast system is adversely affected by relative transmitter and receiver placements and the electronic and physical environment in which it is operating.

In contrast, the intelligent transceiver system of this invention passes messages from sensors directly to base station **12**, or if needed, from sensor-to-sensor to base station **12**. Each sensor passes its message on with a different identifying code or unit address and with a carefully synchronized delay factor so that no two sensors broadcast at the same time. This eliminates a mutual interference, or message contention, problem. The transceiver system is designed so that each sensor delays transmitting a message until its receiver has sampled the airwaves to ensure there is no interference. Preferably this sampling occurs up to six times before triggering an automatic recovery process to reestablish contact through another route. The transceiver system functions from the sensors to the base station **12** or vice versa, attempts different routes to overcome obstructions, and dynamically reconfigures its routing to circumvent problems. The maximum communications range between low-power wireless sensors is typically about fifty meters (150 feet) indoors, and the effective range of an entire system can be up to about 2.5 kilometers depending on the number of sensors. Because each sensor requires very low power to reach its neighboring sensors, power consumption is lower compared with conventional systems that must transmit at higher power to reach longer ranges.

Conventional one way radio systems control employing a transmitter in each sensor and a receiver in the base station are relatively inexpensive to manufacture. However, when problems occur it is impossible to interrogate a sensor to check its status. Moreover, if no signal is received from a sensor, it is impossible to determine from the base station whether the sensor has encountered an obstruction or has some other problem, such as a depleted battery. Likewise, if the sensor transmits its message, it cannot determine whether the message was received by the base station. This is referred to as a "Shout and Pray" communications principle. Accordingly, messages are typically transmitted repeatedly to improve the chances of successful reception.

However, in the transceiver based alarm system **10** of this invention, a sensor transmits its message once, and repeats the message only if the first transmission is not acknowledged. This method significantly reduces the transmission time required, as well as the current consumption needed, which improves the battery life.

The intelligent transceiver architecture of this invention employs a two-way message exchange, which allows interrogation. Base station **12** routinely checks whether a sensor is active and double checks in the event of problems. The sensors also use the two-way link to confirm successful transmission of messages. Thus, the two-way message exchange provides a more reliable communication method, and it also enables passing messages from base station **12** to the sensors to provide a wider range of system monitoring functions.

Alarm system **10** includes a microprocessor in base station **12** and every sensor. The microprocessors employs this "distributed intelligence" as follows: Each sensor checks that its messages are acknowledged by base station **12**. If the messages are not received, the sensor automatically reconfigures until the message is acknowledged. Each sensor reports problems, such as low batteries, by monitoring power usage and a series of other performance checks. Each sensor double checks any detected problems. Alarm conditions can be verified to reduce the number of false alarms. Transceivers can be switched on and off to minimize power consumption. Sensors can be remotely instructed to turn on or off, when the security system becomes armed or disarmed, to minimize power consumption and reduce message clutter. The sensors can be remotely instructed to carry out further functions, such as system extensions or installation of new performance requirements.

Conventional transmitters employ a fixed frequency. If noise or interference occurs on that frequency, then transmitted messages may be distorted or lost. Such interference is very common and constitutes a major cause low reliability in conventional radio systems.

Prior workers have tried to find solutions to interference and jamming problems. Some employ protocols to send each message multiple times, and others use two transmitters in each unit to redundantly transmit the message on two frequencies at the same time. However, this is an expensive and cumbersome solution that does not always work. Spread spectrum technology is sometimes seen as a practical, though expensive solution. Even if one or more of the frequencies within its spectrum is occupied at the time of message transmission, the system relies on the remaining spectrum to sufficiently transmit enough of the message to the base station. In such conventional systems, no alarms are triggered unless the base station determines that the received messages are accurate. Indeed, many systems are deliberately set so that if any doubt exists, no alarm is triggered.

However, in this invention, a sensor does not transmit a message until it has sniffed the airwaves to check for interference up to six times in a maximum of 750 milliseconds before reporting back to base station **12** that transmission is presently impossible on the present frequency. Once alarm system **10** determines that the present frequency is subject to interference, it finds another frequency that is interference free and switches all the sensors to the new frequency. By changing frequency channels when interference is detected, a much more reliable system is realized. It is also common to place a device at a location subject to multipath cancellations that prevent messages from being reliably received. Solutions to this problem include employing multiple receivers and changing frequencies.

Changing among multiple frequency bands has additional advantages. Although communications can occur between sensors and base station **12** on one frequency, this invention employs one frequency for devices, another frequency for base station **12** and, in some applications, a third frequency for the autodialer or communications to a central monitoring station. When downloading information from a remote location to alarm system **10**, long messages may be sent from the autodialer to base station **12** or to a sensor that acts as a communications hub. If the long messages were communicated on the same frequency as the sensors, they would all become activated for the duration of the messages, causing unnecessary power consumption. Also, when base station **12** sends messages to the autodialer, the same unnecessary power consumption occurs. Likewise, if any device reports an alarm condition, all other devices would also receive the message, even though the message is meaningful only to base station **12**.

Referring to FIG. **2**, in apartment and dormitory applications, a single base station **12** in one living area transmits a message to an autodialer or to another base station **12** in another living area to pass neighbor watch type information, or to pass that information on to central monitoring station. In this application, all other devices would be required to listen to all of the messages unless different frequency channels are used.

In a meter reading application, a transceiver powered by and attached to the meter, transmits periodically, preferably once every hour, to report power consumption for variable rate billing purposes. If base station **12** employs a separate frequency for this purpose, then only base station **12** will be activated to received this periodic message, thereby conserving the battery life. In general, when messages are frequent or of a long duration, it is preferred to employ separate frequencies.

When a sensor transmits an alarm message to base station **12**, a simple acknowledgment to the sensor from the base station **12** is sufficient to close the communications loop and ensure reliable transfer of critical information. There are, however, cases where this is insufficient.

Most security or fire alarm systems require that all wireless devices be supervised by base station **12** to verify that these devices are still in communication with the base station **12**. Base station **12** is required to verify communications within four hours in most security systems, but as often as four minutes for some commercial fire systems.

In conventional one-way wireless security systems, each transmitter sends a packet of information that includes a supervision message that typically repeats once an hour. When the base station misses receiving four of these messages in a row, a loss of supervision is indicated. Some supervision messages are lost simply because the transmitters all send their messages at random time periods, causing some of them to clash with one another.

However, in the two-way communication system of this invention, supervision messages are communicated by a more orderly polling method. In conventional polling, the base station initiates a poll by first sniffing to verify that no other transmissions are occurring. Then a first sensor is contacted to verify its proper operation. The first sensor acknowledges, and the base station polls the second sensor, and so on. A problem with conventional polling is that the base station must individually poll each sensor, and all of the sensors remain activated for the duration of the complete polling sequence. If 16 sensors are polled, conventional polling requires 16 base station transmissions and 16 individual device acknowledgments, which requires a greater power consumption by the base station than by a sensor.

However, in a group polling method of this invention, a supervision poll request message is transmitted by base station **12** that is recognized by all sensors having a same house code as one embedded in the supervision poll request. Then, the sensors acknowledge after a predetermined time delay related to the unit address of each device. Thus device number one immediately returns an acknowledgment, followed by device number two, then device number three, etc., with each acknowledgment spaced apart in time to avoid clash problems. With the group polling method, base station **12** and the sensors each generate one transmission, thereby reducing power consumption by base station **12** and each of the devices. Group polling is further beneficial because it takes about half the time as conventional polling. To reduce time and power consumption even further, sensors need not respond back with their house code addresses, but only need to report their unit addresses because their timed transmissions confirm the correct house codes.

With group polling, if a sensor does not acknowledge a supervision poll request, base station **12** immediately interrogates that sensor to determine whether it is still active in the system. If base station **12** received no response from the sensor, it may be out of range, so base station **12** requests the other sensors to attempt contacting the nonresponding sensor to determine whether it is present. Therefore, within a few seconds, every sensor should be accounted for. A supervision poll request once every four hours achieves a higher supervision level than conventional polling once an hour from each transmitter.

With group polling, once it is determined by base station **12** that a sensor is out of range, but responds to another sensor, base station **12** stores this information and, in the future, contacts the nonresponding sensor through the intermediate sensor. For example, if sensor number **12** is out of range of base station **12**, but in range of sensor number **5**, base station **12** stores this information and communicates to sensor number **12** through sensor number **5**. This message routing information is also stored in sensor number **12**.

This communication path determining method is preferably accomplished during the initial enrollment of sensors. During the enrollment process, base station **12** contacts each sensor individually; and also contacts each sensor through other sensors until a reliable communications path has been established for each sensor. Once the paths are determined and stored in the station **12**, it downloads to each sensor the best next sensor it communicate with for sending messages, thereby establishing for each sensor a primary communications path. For greater reliability, a secondary path may also be stored. This same process may be repeated whenever enrolling new sensors or if a nonresponding sensor is discovered during a supervision poll sequence.

Other types of group polling messages may also be employed, such as for fire alarms, burglary alarms, medical emergency alarms, panic/hold up alarms, trouble signals, and system arming and disarming. Are all examples of messages that can be sent to all sensors rather than requiring separate communication to each sensor. Three or four separate arming and disarming levels may be employed, such as to indicate whether a system is armed, anyone is at home, when it is armed at night and people are upstairs sleeping, and when a system is armed before an extended vacation. In each case, different sensors might respond differently, such as lights being turned on and off, motion sensors being turned on and off, and the like.

Conventional transmission based alarm systems require either manually assigning addresses for each sensor, such as with dip switches, or employ pre-set mega-addresses in the sensors that must be "learned" by the base station.

However, in the transceiver-based alarm system **10**, only base station **12** is manufactured with a unique pre-set "house code," whereas the sensors have no pre-assigned addresses. When base station **12** is placed in, "enroll" mode and a new sensor is first powered up, then base station **12** recognizes this sensor as new, and downloads to the sensor the house code and a unique sensor address. This makes the enrollment process automatic, without the need for manufacturing sensors with unique codes. This method also allows for shorter sensor addresses than are required for sensors with pre-assigned addresses. Shorter addresses make for shorter, more rapid transmission times, which reduces battery consumption.

Conventional security and fire alarm systems employ control panels to enclose system intelligence, power supplies, wiring interconnections, and the autodialer.

However, the wireless system of this invention does not actually require a control panel because each sensor is battery operated, the system requires no sensor interconnections or wiring hub, the dialer may stand alone or be replaced by a cellular radio link, and intelligence can be located in any sensor or sensors.

Regarding intelligence, a control microprocessor may be located in the dialer unit of a simple fire system, or in a keypad of a security system. If the keypad is eliminated, wireless key fobs may be used for arming and disarming and the control processor, which may be located in any sensor.

Security and Fire Alarm Systems require remote monitoring. In monitored systems, wireless communications may provide a primary or back-up path for reporting alarms. Regulatory codes and standards are established to govern the minimum supervision level required to establish a reliable wireless communications link. For example, some systems require only a monthly test signal for testing the communications path. Other systems, such as monitored commercial Fire Alarm Systems, require daily supervision. Other high security applications, such as monitored security systems in jewelry stores or banks, require supervision as often as every six minutes. Such alarm systems, especially where frequent supervision is required, can be severely burdened by the supervision signals, making costs too high for some wireless technologies, and forcing alternate supervision means.

There are numerous conventional supervision techniques employed by the above monitored systems including, for example, cellular radio, dedicated long-range radio networks, two-way paging systems, dedicated lines, and Derived Communications Channels. The latter two techniques do not employ wireless communication, but are employed where high security is required. All of the above techniques, however, require regular and frequent supervision, which adds significant monitoring service costs.

A supervision technique of this invention adds frequent supervision to a wireless communications path by using cellular, GSM, or PCS technologies, at a significantly reduced cost. This invention also provides significantly improved wireless communications reliability and enables one common radio to provide low or high supervision levels without added manufacturing costs. This invention employs standard cellular radio, GSM, and PCS communications methods in a new way. When a cellular radio, or telephone is first turned on, a registration signal is sent by the radio to the nearest cell site to communicate a unique radio identification number, the radio phone number, and roaming data if the radio is outside the home area code. This information is returned to a Central Office located in the area code of the telephone to notify the Central Office that the radio is on and available for calls. The information also identifies the cell site in which the radio is located.

When the radio, or telephone, originates a call, a phone call request signal is forwarded to the Central Office where the radio is verified as a valid radio and the account is checked to ensure that the radio is authorized and paid up. If it is, a message is returned to the cell site and to the radio, opening a voice channel for placing the call.

The registration and call request signals employ special "control" channels, while the telephone call itself is communicated via different "voice" channels. The control channels send very short data bursts containing information such as radio ID, phone number, roaming data, cell site, etc. Voice channels are designed to carry much longer transmissions, such as voice and computer data.

Until recently, almost all billing charges have been based on voice channel usage. Some new technologies, such as Cellemetry and Microburst, employ the control channels to send short data messages, such as alarm or monitoring information. However, none of these technologies uses the registration signals to provide supervision.

When a cellular radio is turned on, it not only transmits a registration signal, but also regularly makes registrations thereafter at varying times, such as from every few minutes, up to 60 minute intervals. This verifies that the radio is still on and in the same cell site. Registrations stop when it is determined that the radio is no longer responding because it has been turned off, is out of range, or moved to a different cell site. The registration process is repeated if the cellular radio moves to a new cell site.

The registration process occurs continually for all cellular radios that are turned on. However, cellular service providers do not charge for registration because they are considered a required part of the rapid call placement infrastructure.

Accordingly, this invention employs registration signals to supervise the communications link with the radio. The registration signals are conveyed from the Central Office to a processor and are analyzed to verify continuous connectivity. This method, therefore, adds no extra call request demand on the cellular radio network or infrastructure yet provides improved supervision. For example, 15 to 30 minute registration intervals are common for stationary radios (more often if mobile). This is far greater than the once-a-day supervision required by commercial Fire Alarm Systems, without the need to initiate daily call requests.

Because the cellular radio initiates registration signals, such as when first turned on, the radio can be designed to generate more rapid registration signals, such as once every 5 minutes, when needed for high-security applications. This slightly increases the number of registration messages sent, but it is still well below the typical registration rates for mobile radios caused by the relatively rapid movement from cell site to cell site.

Therefore, the cellular radio is designed to generate registration messages every 5 minutes, if needed for high-security applications. When high security is not needed, the radio relies on the lower registration rates requested by cell sites.

The cellular radio requests an acknowledgment from the cell site when the registration signal is initiated by the radio and checks for the regular registration signal when it is initiated by the cell site. In this way, the cellular radio can detect when a cell site call connection is lost and generate a communication trouble signal. The trouble signal may alert people on the local premises, via audible or visual signaling means, or can be transmitted back to the Central Monitoring Station by a second telephone line or communications path if available. A second telephone line is required in commercial fire and high-security applications.

This invention is further advantageous when employed with the newer control channel data communications technologies and, in particular, with Microburst. This is because collecting registration signals from the Central Offices and forwarding them to a processing center for supervision purposes is not a simple matter when Central Offices throughout the country might be involved.

However, because Microburst Technology employs a single central office, or hub, for all Microburst radios, all registration signals and control channel data from call requests can be collected in the central office. Therefore, the registration signals are readily conveyed along with the control channel data to a processing center for supervision.

If the processing center detects a loss of supervision of registration signals, this information is conveyed to a monitoring center for notification of the proper authorities.

Skilled workers will recognize that this communication in supervision technique is useful for other applications, such as meter reading, vending machine monitoring, and mobile vehicle tracking.

Employing transceivers **32** and **60** and communications protocols of this invention allow wireless alarm system **10** to match the performance of wired alarm systems while providing the advantages of simple installation, low cost, improved in-service performance, higher reliability, and added user benefits.

FIG. **6** shows transceiver **60**, which is preferred for use not only in sensors, but in place of transceiver **32** in base station **12** because it enables implementing an micro-power, asynchronous, two-way, radio frequency data network with a special wake-up protocol. Transceiver **60** can also be applied for point to point radio frequency communications for extending battery life, such as in cordless phones and wireless keypads.

Transceiver **60** overcomes the many constraints to extending battery life and maintaining reliable radio data communication under a network condition. Transceiver **60** includes a microprocessor **70**, which is preferably a Texas Instruments MPS430 ultra-low power processor with on-chip memories. An additional non-volatile memory may be required for storing personalized network information.

Transceiver **60** further includes a transceiver chip **72** that integrates most circuitry for a local oscillator, phase locked loop, in-channel and quadrature-channel data paths, RF and IF filters, and a base band control circuit. Transceiver chip **72** is preferably a type number NOVA3.3 available from Gran-Jansen of Oslo, Norway. Transceiver chip **72** communicates serially with microprocessor **70** to select sleep, receive, and transmit modes; transfer control data; transfer receive and transmit data; and setup and phase-lock associated frequencies. A varicap **74** receives modulation data through a filter network **76** to frequency shift key ("FSK") modulate data in transmit mode.

Transceiver chip **72** employs a stable 10 MHZ crystal **78** and digitally synthesizes frequencies under shared phase-lock control with microprocessor **70**. Transceiver chip **72** need not have a fast wake-up time nor particularly low power consumption because it is in sleep mode a majority of the time. An antenna **79** is coupled through resonant circuits to the RF in and out pins of transceiver chip **72**.

Transceiver **60** also includes a superregenerative micro-power receiver **80** that incorporates a sampling mixer. Micro-power receiver **80** draws only about one to six microamperes of current during sleep mode and includes a Colpitts oscillator **82**, a quench oscillator **84**, a pulse-forming network **86**, a signal extraction network and data interface **88**, and an antenna **90**. Alternatively, micro-power receiver **80** may be coupled to antenna **79**. A suitable implementation of micro-power receiver **80** is described in U.S. Pat. No. 5,630,216 for MICROPOWER RF TRANSPONDER WITH SUPERREGENERATIVE RECEIVER AND RF RECEIVER WITH SAMPLING MIXER, which is incorporated herein by reference.

Battery power for transceiver **60** is received through a connector **92** that also transfers receive and transmit data with the sensor or control unit in which it is installed. Monitoring battery condition is an important function that is carried out during every message transmission (the highest current drain condition) by transceiver chip **72** to ensure reliable sensor or base station **12** operation.

Microprocessor **70** includes a digitally controlled oscillator ("DCO"), a predetermined frequency of which decreases as the battery voltage decreases. A reference frequency is established by a stable 32.768 KHz crystal resonator **94**. Comparing the DCO predetermined frequency to the reference frequency provides a means for monitoring the battery voltage.

Microprocessor **70** performs numerous functions including decoding a specially coded "wake up" message received from micro-power receiver **80**; formatting and Manchester encoding data during transmit mode; performing frame, packet, byte, symbol, and bit synchronization; performing received signal strength measurement during receive mode; and controlling media access layer and logical link layer protocols.

The media access layer control includes sleep/wake-up cycle control, data collision control and media access layer acknowledgment. The key media access method employs a combination of an ALOHA protocol approach during wake-up sequences and carrier sense multiple access/collision avoidance ("CSMA/CA") after wake-up sequences.

The logical link control includes device addressing; packet structure; packet error control; and network layer functions, such as RF channel control, packet routing, routing table management, and supporting mobile devices for roaming in and out of the coverage area. Microprocessor **70** can receive external triggers in sleep mode, and passes all the data associated with high layer protocols to a processing unit in the associated sensor or base station **12**.

To achieve reliable two-way communication through a wireless data network, periodic synchronization of the network must be accompanied by a quick network response. This is difficult to achieve in networks in which all the sensors and base station **12** are battery powered. Features such as packet routing, channel switching (to avoid RF interference and jamming) and roaming for mobile devices (i.e., the device is out of reach of the network during normal operation) place additional demands on the battery capacity and add complexity to the communication protocols. Moreover, with some communication protocols, the need for fast transceiver wake-up and low power operation make the transceiver design challenging.

The above-described communication protocol employs a low duty cycle of message transmitting time compared to the standby time. Accordingly, the network is in a sleep mode most of the time. Unfortunately, this makes network synchronization difficult. Therefore, transceiver **60** employs the following cascaded wake-up communication protocol.

When no messages are being transmitted, all sensors and base station **12** are in an ultra low power sleep mode. During sleep mode, micro-power receiver **80** monitors a predetermined frequency, preferably 418 MHZ in the United States and 433 MHZ in Europe. Micro-power receiver **80** can be very simple because it is not required for data communication, only for receiving the "wake-up" message.

Whenever any of the sensors or base station **12** need to send a message, its transceiver chip **72** first transmits the wake-up message.

All other sensors and base station **12** receive and decode the wake up message via their micro-power receivers **80**, which in turn wakes up microprocessor **70** to redundantly decode the wake-up message to determine whether to activate transceiver chip **72**. If a wake-up message is definitely received, microprocessor **70** deactivates micro-power receiver **80** and activates transceiver chip **72**.

After the sensor sends the wake-up message, it transmits a synchronization sequence, to synchronize the other transceivers in alarm system **10**.

Following the synchronization sequence, a data message can be transmitted to an individual address or broadcast to a group addressed devices.

A confirmation message is returned by the addressed device or devices.

Upon completing communications, all sensors and base station **12** return to the sleep mode to extend battery life.

To implement the wake-up message, transceiver **60** emulates a low speed amplitude-shift keyed transmission. All transceivers employ the same predetermined frequency for transmitting and receiving wake-up messages. Emulating the low speed transmission requires switching the transmitter on and off at a controlled rate, preferably less than 1 KHz, which limits the wake-up message bit rate to less than 1 kilobit per second. Slower speeds can be employed as long as micro-power receiver **80** can reliably decode the wake-up message. Microprocessor **70** requires a fast wake-up time, preferably less than a few microseconds, to properly process the wake up message. The wake-up message includes the system number to determine which systems are to wake up.

To implement the data communication protocols, transceiver **60** switches to a 19.2 kilobaud, Manchester coded, FSK mode for transmitting and receiving data. Data communication frequencies are readily switchable among numerous channels in a 400 MHZ range or a 800 MHZ range. The preferred channel bandwidth is 60 KHz and the channel spacing is 120 KHz to avoid adjacent channel interference. Before each data transmission, a series of Manchester zero codes are transmitted to ensure communication frame synchronization. Packet start and end sync words inserted to enable packet synchronization. Byte synchronization is employed to avoid sampling clock drift problems. Element/bit synchronization is achieved by recovering the sampling clock frequency from the sequence of Manchester coded zeros. The communication protocol operates in half-duplex mode.

The wake-up protocol enables using a very simple medium access control method with no regular system synchronization being necessary. Preferred medium access control parameters are described below.

The wake up message is the same for all systems and is transmitted on a predetermined frequency.

The wake up message is one way only and is transmitted by any device that awakens from sleep mode to transmit a data message.

Normal half-duplex data communication is carried out on a frequency that is established during system set up, log on, or during enrollment.

After any of the sensors or base station **12** awakens, it shall not listen for a further wake up message.

Each data message, transmitted after the wake up message contains a frame synchronization preamble comprising a series of Manchester coded zeros.

All data messages are acknowledged by the addressed device.

If the acknowledgment is missing, an RF message collision is assumed. A retransmission is attempted at least three times or until a valid acknowledgment is received.

Any sensor or base station can transmit a data message after the first data message, but it must first listen to ensure the channel is clear before switching from receive to transmit mode.

Transceivers wait in receiving mode until the channel is clear.

To avoid further RF collisions, a random delay is applied before attempting a re-transmission.

Sensors and control units return to sleep mode after sensing a clear RF channel for a predetermined time.

The following alternative communication protocol is preferred when employing transceiver **32** or transceiver **60** without micro-power receiver **80**. The alternative protocol employs half duplex, Manchester coded, FSK data communication at 19200 kilobaud, eight frequency channels for either US or European markets, and a reserved frequency for one-way transmitting devices, such as for transmitting the wake-up message. The frequency spacing is 200 KHz.

A combination of frequency division multiple access and time division multiple access communication methods are employed. Alarm system **10** communication synchronization employs a deterministic non-contention technique in which base station **12** synchronizes the system every **60** during a one second active time interval. Cross system contention is possible if two systems are using the same RF channel. If a collision occurs, base station **12** sets a random number between 30 and 60 seconds for the next system synchronization. Up to 30 systems can co-exist on a single RF frequency with a 33 millisecond time slot for each system. The systems uses CSMA/CA protocol to reduce collisions during half duplex operation. Each message is acknowledged by its addressed recipient, which serves as a basis for collision detection.

Cross system communication is possible if two base stations are within communication range. The special RF channel is used for cross system communication, so each base station must monitor its own frequency and the special frequency during every wake-up time period. One hundred systems may co-exist within one RF range, which is typically 100 meters in free space and 50 meters indoors. Accordingly, any sensor can transmit a "find base station" message if does not detect its own base station during a predetermined time interval.

Transceivers **32** and **60** can relay messages to three other transceivers that are outside the range of base station **12**.

Up to 32 transceivers may be assigned to an addressable group, and 32 groups are assignable.

The following communication protocol is employed to ensure system synchronization and minimize collisions.

Each sensor is monitoring its own pre-assigned frequency, and base station **12** monitors both its own assigned frequency and the special frequency.

Alarm system **10** is awakened once each second to listen for any possible messages or extraneous radio-frequency activity.

A preferred wake up sequence for transceiver **60** is: microprocessor **70** awakens and activates transceiver chip **72**. Transceiver **60** then performs oscillator and phase-locked loop stabilization and lock. Once locked, transceiver **60** cycles through a number of 104 microsecond time slots for performing respective, frequency monitoring, base station **12** detection, odd numbered logical address detection, even numbered logical address detection, frequency monitoring, and returning back to sleep mode.

After monitoring its own assigned frequency, base station **12** sends an 82-bit control word to its transceiver chip **72** to switch to the special frequency. After frequency locking, transceiver chip **72** monitors the special frequency for 520 microseconds before receiving another 82-bit control word for switching to the next active time slot before returning to sleep mode.

An "acknowledgment" message is transmitted within one millisecond by a transceiver in response to receiving any message from another transceiver. If the acknowledgment is missing, a message collision or jamming is assumed. Three retransmissions are attempted before transceiver **60** reports the missing acknowledgment to its local host processor. Acknowledgments have the highest processing priority.

Time slot synchronization is carried out once per minute by base station **12** transmitting a five millisecond synchronization burst. Each sensor wakes-up 33 milliseconds. If any sensor is not correctly time synchronized and, consequently misses the synchronization burst, its next wake-up time slot is begins five milliseconds earlier and ends five milliseconds later. If the sensor misses three successive synchronization bursts, this fact is reported to its local host processor, and the sensor transmits a "find base station" message.

Alternatively, the synchronization burst may be transmitted more often, for example, once every two to ten seconds to provide tightly synchronized communications among devices. However, this causes increased power consumption and communications traffic.

The synchronization burst may also be transmitted less often, for instance once per hour, which is the time period for normal application supervision. This reduces power consumption and communications traffic, but a very long synchronization burst may be required.

Data messages transmitted in alarm system **10** are acknowledged by the receiving device transmitting an "application acknowledgment" message. The addressed and acknowledging devices stay awake, and the other devices return to sleep mode.

Alarm system **10** further performs two network service functions. One is determining message routing when it is necessary to relay a message from a transmitting device, through at least one intervening device, to a message receiving device. The other function is establishing cross system communications under special alarm conditions, such as when base station **12** is inoperative.

Message routing requires flexibility because there are a number of factors affecting communications, such as: moving a device; modifying building construction or moving furnishing and, thereby, causing multi-path signals that weaken reception; or introducing a source of interference.

Message routing employs a automated Pathfinder® protocol that accounts for the above changing communications environment. The Pathfinder® protocol employs setup, operation, and reset phases.

In the Pathfinder® setup phase, each device expects a supervision poll from base station **12**, or another domain controller, every hour or 72 minutes. For the synchronous data network embodiment, a network devices expect a synchronization burst every minute. These regular communications could be missed because of degraded communications conditions. Under such circumstances, the affected device broadcasts a "find base station" command. Any other devices in the same network can accept this command and relay the message to base station **12** and reply to the initiating device. The initiating device thereby learns that it is not directly communicating with base station **12**.

Once base station **12** receives the "find base station" message, it creates a routing; table and nominates a suitable router or routers for communicating with the initiating net device. The routing pathway will be one of the relay pathways taken by the "find base station" message. Base station **12** determines the easiest and most reliable path stored in the existing network configuration and routing tables.

Once a routing pathway has been established, base station **12** downloads the routing table to the router(s). The routing table includes the unit address of each device and a group number.

The Pathfinder® operation phase proceeds as follows: Once a device has a non-empty routing table, it takes on the added function of a router. Messages between base station **12** and final designated devices have the same structure (source address and destination address, or group number) as a broadcast message. The router determines whether to relay or discard a message.

When a device receives a message, it checks the destination address to determine whether the message requires routing. If the destination address does not matches its own unit address, the device checks its routing table unit addresses, and if a match is found, the router relays the message without modification.

For a broadcast message, the router examines the group number against the routing table regardless of its own group number status. The message is relayed without modification if a match is found in the routing table.

If the destination address is the base station address, the source device address is checked against the routing table. If a match is found, the message is relayed without any changes.

Messages from base station **12** to the final designated devices or vice versa are preserved during relay operations and are "transparent" to ensure the correct source and destination unit addresses.

Pathfinder® reset phase operates as follows: Base station **12** may receive multiple replies from a final designated device including a very fast message acknowledgment from the device. This indicates that direct communication is possible. Base station **12** can then download an updated routing table to the previously defined router(s) or clear items in the routing tables. This changes the routing pathways and resets the previous router.

There are many advantages to the two-way wireless alarm system described herein versus prior one-way wireless alarm systems.

When an alarm is detected by any sensor, all sensors sound the alarm so it can be heard throughout the house.

To silence a fire alarm, pressing the "Silence" button on any smoke detector silences all the sounders.

To set up and test this two-way system, a user presses the "Enroll" button on the base station **12**, and places batteries into each sensor. Then, pressing one of the "Test" buttons tests the whole system.

Adding a two-way security system to an existing fire system only requires adding a two-way wireless keypad and two-way wireless security sensors in communication with the keypad. The keypad then reports through the autodialer.

The cost of a one-way smoke detector is less than the cost of a two-way smoke detector. However, the cost of a one-way base station is higher than the cost of two-way base station **12** because a dual diversity receiver is required in the one-way unit to provide reliable reception. Moreover, the receiver must operate continuously, thereby requiring an AC power adapter, a voltage regulator, added lightning protection, and back-up batteries.

Because an AC power adapter is needed for a one-way system, the homeowner will be required to connect the base station to an unswitchable AC power source, which is not always close to a telephone jack.

In the two-way system, transmission range is not limited by the distance between the base station **12** and the most distant sensor because messages are relayed from sensor to sensor.

In the two-way system, during trouble conditions, such as a low battery or dirty detector, such trouble conditions are indicated only at base station **12** until its door is opened, at which time base station **12** signals the appropriate detector to indicate its trouble condition.

Communications reliability is higher in a two-way system because sensors receive acknowledgment that alarm messages have been received, or the system can retry message transmission on multiple frequencies, or via alternate paths, until an acknowledgment is received.

Complete elimination of wires is possible in a two-way wireless system, enabling much easier and quicker installations and requiring less technical aptitude and training to complete.

Of course, one-way communications may be employed in selected low-cost sensors to suit particular application requirements.

It will be obvious to those having skill in the art that many changes may be made to the details of the above-described embodiments of this invention without departing from the underlying principles thereof. Accordingly, it will be appreciated that this invention is also applicable to wireless control applications other than those found in alarm systems. The scope of this invention should, therefore, be determined only by the following claims.

What is claimed is:

1. A method of automatically programming a wireless sense and/or control system to enroll one or more sensor devices distributed at different locations throughout a spatial region, comprising:

providing a two-way wireless communication capability between a base station having a base station transceiver and at least one of the sensor devices having a sensor device transceiver;

initiating an enroll condition in the base station to place the system in a sensor device enroll mode;

introducing a trigger event to a sensor device and delivering from the sensor device transceiver to the base station transceiver in response to the trigger event a new device message signal identifying the sensor device;

delivering from the base station transceiver to the sensor device transceiver in response to the new device message signal a programming signal indicating a sensor device address; and

storing the sensor device address in the sensor device.

2. The method of claim **1** in which the programming signal further comprises system configuration information that includes one or more of sensor device addresses of other sensor devices in the system, a signal transmission frequency, and communication pathway information relating to communication between the base station and any of the sensor devices enrolled in the system.

3. The method of claim **1** in which the sensor device is out of direct communication range with the base station, and further comprising an intervening sensor device having an intervening sensor device transceiver positioned to receive from the sensor device and transmit to the base station the new device message signal and to receive from the base station and transmit to the sensor device the programming signal.

4. The method of claim **3** in which the spatial region comprises a multi-dwelling complex, the base station is installed in communication with the multiple dwelling complex, and the sensor devices are installed in individual dwelling locations.

5. The method of claim **1** in which the introducing a trigger event to a sensor device comprises installing a battery in the sensor device.

6. The method of claim **1** in which the base station is battery powered.

7. A low power sense and/or control system implemented with wireless two-way communication capability in a communication medium between a base station and one or more of multiple sensor devices distributed at different locations throughout a spatial region, comprising:

multiple sensor devices each having a different identification address and a sensor device transceiver that transmits a communication message signal in response to a wake-up producing condition, the sensor device transceiver including low power-consuming sensor signal processing circuitry and sensor signal communication circuitry selectively switchable between a lower power-consuming standby mode and a higher power-consuming operating mode, and the sensor signal processing circuitry storing in memory sites different control signals corresponding to different communication message signal producing conditions; and

a base station having a base station transceiver including base station signal processing circuitry and base station signal communication circuitry, the base station signal processing circuitry cooperating with the base station signal communication circuitry to receive the communication message signal and transmit in response to it an activation signal to which the sensor device transceiver of the sensor device that transmitted the communication message signal can respond to produce a control signal corresponding to the communication message signal producing condition, and the base station receiving from the sensor device transceiver that transmitted the communication message signal a supervision message that includes the identification address to verify a communication link between them.

8. The system of claim **7** in which the base station signal communication circuitry is selectively switchable between a lower power-consuming standby mode and a higher power-consuming operating mode and in which the base station further comprises a micro-power receiver in operative association with the base station transceiver, the micro-power receiver communicating with the base station transceiver such that, in response to detection by the micro-power receiver of the communication message signal, the base station signal communication circuitry assumes its operating mode to enable the base station transceiver to decode the communication message signal and transmit the activation signal to the sensor device that transmitted the communication message signal.

9. The system of claim **8** in which each of the multiple sensor devices further comprises a micro-power receiver in operative association with the sensor transceiver, the micro-power receiver communicating with the sensor transceiver such that, in response to detection by the micro-power receiver of the communication message signal, the sensor transceiver assumes its operating mode to receive the activation signals.

10. The system of claim **8** in which, after the base station signal communication circuitry assumes its operating mode, the base station transceiver receives a portion of the communication message signal to confirm that the signal detected by the micro-power receiver is a valid communication message signal.

11. The system of claim **8** in which the base station transceiver transmits the control signal to multiple sensor devices in addition to the sensor device that transmitted the communication message signal to provide at different locations in the spatial region the control signal of the communication message signal producing condition.

12. The system of claim **7** further comprising an automatic telephone dialer that is operatively connected to the base station for communicating with a monitoring center in response to at least one of a test condition, a trouble condition, an alarm condition, a sensor device supervising process, a base station-to-monitoring center supervising process, a verification process, or a status indicating condition.

13. The system of claim **7** in which one of the multiple sensor devices is an out-of-range sensor device that is out of direct communication range with the base station, and further comprising an intervening sensor device having an intervening sensor device transceiver positioned to receive from the out-of-range sensor device and transmit to the base station the communication message signal and to receive from the base station and transmit to the out-of-range sensor device the activation signal.

14. The system of claim **7** in which the base station signal communication circuitry is selectively switchable between a lower power-consuming standby mode and a higher power-consuming operating mode and the base station signal communication circuitry assumes its operating mode during a time when the sensor device transmits the communication message signal to receive the communication message signal and transmits in response to it an activation signal to which the sensor device transceiver of the sensor device that transmitted the communication message signal can respond to produce a control signal corresponding to the communication message signal producing condition.

15. The system of claim **7** in which the base station transceiver continually transmits synchronization signals and in which the sensor signal communication circuitry of each of multiple sensor devices continually switches between the standby and operating modes to sample the communication medium for transmission of the synchronization signals and thereby enable the sensor device transceiver in its operating mode to receive the synchronization signals, to thereby enable synchronization of the switching between the standby and operating modes of the multiple sensor devices.

16. The system of claim **7** in which the sensor signal processing circuitry of each of the multiple sensor devices establishes a transmission time at which the communication message signal is transmitted, the transmission time of any one of the multiple sensor devices being different from the transmission time of any other one of the multiple sensor devices.

17. The system of claim **16** in which the transmission time of any one of the multiple sensor devices is determined by the identification address of the sensor device.

18. The system of claim **8** in which the base station transceiver transmits the control signal to multiple sensor devices in addition to the sensor device that transmitted the communication message signal to provide at different locations in the spatial region the control signal of the communication message signal producing condition.

19. The system of claim **7** in which the communication message signal producing condition includes a test condition, a trouble condition, an alarm condition, an enrollment process, a supervising process, a verification process, a status indicating condition, a sound-controlling condition, a sensor arming condition, a sensor disarming condition, an indicator light controlling condition, a switch controlling condition, a communication message signal acknowledgment condition, a system configuration indicating condition, or a message routing condition.

20. The system of claim **7** in which the base station is battery powered.

21. The system of claim **7** in which the multiple sensor devices further comprise associated sounders and at least one of the multiple sensor devices transmits a communication message signal indicating an alarm condition, and in which the base station responds to the alarm condition message by transmitting a sounder activating message signal to the multiple sensor devices to sound their associated sounders.

22. The system of claim **21** in which the multiple sensor devices are of a smoke detector type or a fire detector type.

23. The system of claim **21** in which the alarm condition message is a smoke or fire alarm condition message and in which the base station responds to the smoke or fire alarm condition message by transmitting a message resetting the sensor device that transmitted the smoke or fire alarm condition message, and waiting a predetermined time period to determine whether at least one additional occurrence of the smoke or fire alarm condition message is received from any of the multiple sensor devices before transmitting the sounder activating message.

24. The system of claim **21** in which the multiple sensor devices are of a smoke detector type or a fire detector type and in which the base station and each of the multiple sensor devices includes a manually operable button for initiating a silence message that is transmitted throughout the spatial region to silence the sounders.

25. The system of claim **7** in which the multiple sensor devices further comprise associated sounders and one of the sensor devices transmits a communication message signal indicating an alarm condition that the base station fails to acknowledge, the one of the sensor devices responding by transmitting a sounder activating message signal directly to the multiple sensor devices to sound their associated sounders.

26. The system of claim **7** in which the multiple sensor devices are fire, smoke, or intrusion sensor devices that further comprise associated speakers and in which one of the multiple sensor devices transmits an alarm condition message signal to which the base station responds by transmitting a speaker activating message instructing the multiple sensor devices to vocally announce a location of the sensor transmitting the alarm condition message and whether the alarm condition is a fire, smoke, or intrusion alarm condition.

27. A method of automatically programming a wireless sense and/or control system to enroll one or more sensor devices distributed at different locations throughout a spatial region, comprising:

providing a two-way wireless communication capability between a base station having a base station transceiver, an intervening sensor device having an intervening sensor device transceiver, and at least one of the sensor devices having a sensor device transceiver that is out of direct communication range with the base station;

initiating an enroll condition in the base station to place the system in a sensor device enroll mode;

introducing a trigger event to the sensor device and delivering from the sensor device transceiver, through the intervening device transceiver, to the base station transceiver in response to the trigger event a new device message signal identifying the sensor device;

delivering from the base station transceiver, through the intervening device transceiver, to the sensor device transceiver in response to the new device message signal a programming signal indicating a sensor device address; and

storing the sensor device address in the sensor device.

28. The method of claim **27** in which the programming signal further comprises system configuration information that includes one or more of sensor device addresses of other sensor devices in the system, a signal transmission frequency, and communication pathway information relating to communication between the base station and any of the sensor devices enrolled in the system.

29. The method of claim **27** in which the spatial region comprises a multi-dwelling complex, the base station is installed in communication with the multiple dwelling complex, and the sensor devices are installed in individual dwelling locations.

30. The method of claim **27** in which the introducing a trigger event to a sensor device comprises installing a battery in the sensor device.

31. The method of claim **27** in which the base station is battery powered.

* * * * *

EXHIBIT 2

US007262690B2

(12) **United States Patent**
Heaton et al.

(10) **Patent No.: US 7,262,690 B2**
(45) **Date of Patent: Aug. 28, 2007**

(54) **METHOD AND SYSTEM FOR MONITORING EVENTS**

(75) Inventors: **Michael Heaton**, Wingrave (GB); **Jonathan Beardmore**, Wingrave (GB); **Andrew Eccleston**, Wingrave (GB)

(73) Assignee: **Mygard PLC**, Buckinghamshire (GB)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 385 days.

(21) Appl. No.: **10/470,542**

(22) PCT Filed: **Jan. 30, 2002**

(86) PCT No.: **PCT/GB02/00417**

§ 371 (c)(1), (2), (4) Date: **May 13, 2004**

(87) PCT Pub. No.: **WO02/061706**

PCT Pub. Date: **Aug. 8, 2002**

(65) **Prior Publication Data**

US 2004/0189460 A1 Sep. 30, 2004

(30) **Foreign Application Priority Data**

Jan. 30, 2001 (GB) 0102355.5

(51) **Int. Cl.**
G08B 23/00 (2006.01)

(52) **U.S. Cl.** **340/500**; 340/531; 340/506; 340/539.25

(58) **Field of Classification Search** 340/500, 340/531, 506, 514, 539.1, 539.25, 573.1, 340/5.8; 348/148
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,141,006 A 2/1979 Braxton

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0295146 A 12/1988

(Continued)

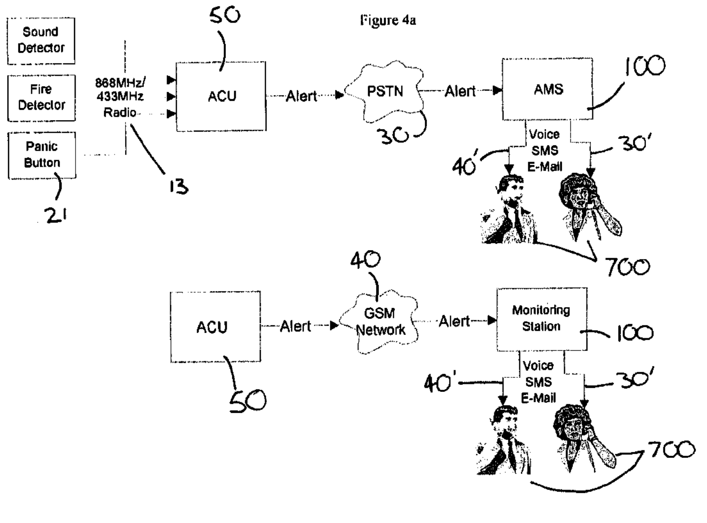
Primary Examiner—Anh V. La
(74) *Attorney, Agent, or Firm*—Fay Sharpe LLP

(57) **ABSTRACT**

The invention provides a monitoring and control system comprising a control unit (**50**) for receiving signals from a variety of detection devices (**10**, **21**, **502**) monitoring events pertaining to security. The control unit (**50**) transmits information related to the reception of such signals to a remote monitoring station (**100**) that stores and operates automatic evaluation routines to send an alert call to a chosen remote user terminal. The remote user terminal may conveniently be a PC, a PDA, a mobile phone or WAP enabled mobile phone, or a fixed line telephone. In some embodiments of the invention it may be possible to provide the monitoring station (**100**) with transmitted information including verification of the event. The nature of the event and verification may be determined by the control unit (**50**) or by the monitoring station (**100**). The invention also provides a control unit (**50**) for receiving alarm signals generated by detection devices (**10**, **21**, **502**) in response to detectable events, the control unit comprising interface unit (**51**) for receiving generated signals and a unit for transmitting information relating to the generated signals (**500**, **501**, **510**, **519**) to a remote monitoring station (**100**).

35 Claims, 6 Drawing Sheets

System Overview



U.S. PATENT DOCUMENTS

4,257,038	A	3/1981	Rounds et al.
4,520,503	A	5/1985	Kirst et al.
4,581,606	A	4/1986	Mallory
5,023,901	A *	6/1991	Sloan et al. 379/38
5,319,698	A	6/1994	Glidewell et al.
5,334,974	A	8/1994	Simms et al.
5,446,445	A	8/1995	Bloomfield et al.
5,499,196	A *	3/1996	Pacheco 702/81
5,651,070	A	7/1997	Blunt
6,040,770	A *	3/2000	Britton 340/539.24
6,246,320	B1 *	6/2001	Monroe 340/506
6,975,220	B1 *	12/2005	Foodman et al. 340/531

FOREIGN PATENT DOCUMENTS

EP	0 308 046		3/1989
EP	0591585	A	4/1994
FR	2661023	A	10/1991
FR	2793334	A	11/2000
GB	2 273 593		6/1994
GB	2 324 630		10/1998
GB	2335523	A	9/1999
GB	2 349 293		10/2000
GB	2 370 400		6/2002
WO	WO96/36301		11/1996

* cited by examiner

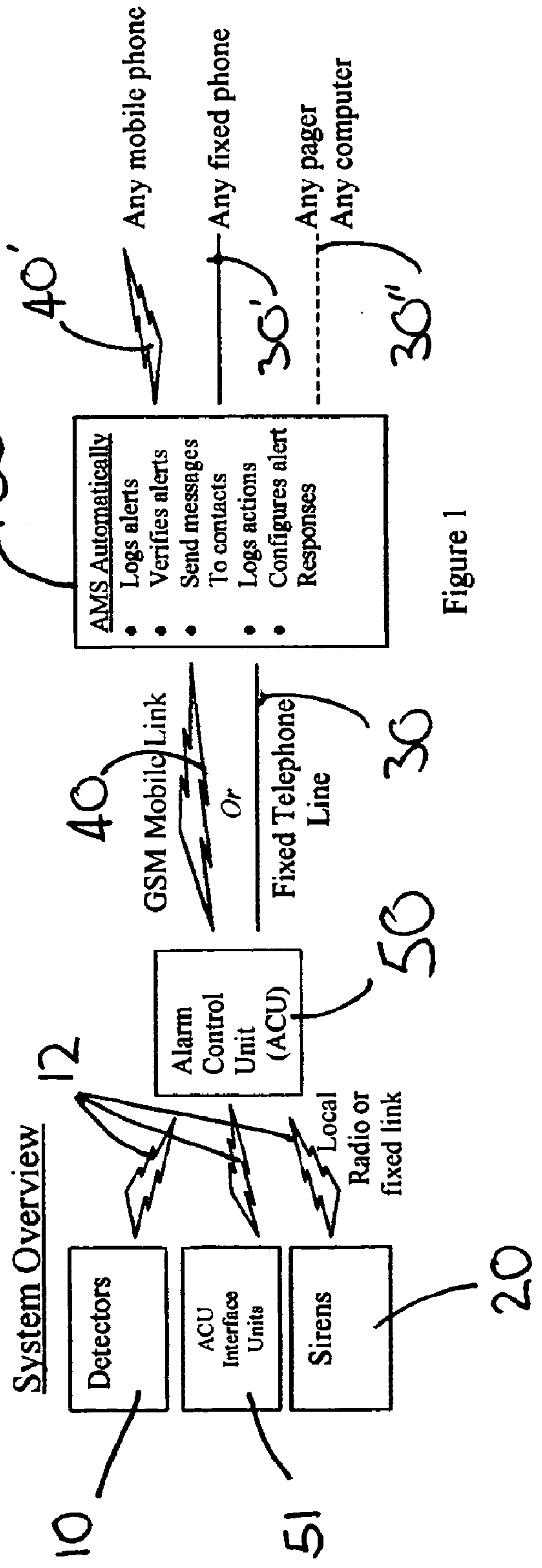

System Overview
Detectors
ACU Interface Units
Sirens
Local Radio or fixed link
Alarm Control Unit (ACU)
GSM Mobile Link
Or
Fixed Telephone Line
AMS Automatically
• Logs alerts
• Verifies alerts
• Send messages To contacts
• Logs actions
• Configures alert Responses
Any mobile phone
Any fixed phone
Any pager
Any computer
10
51
20
12
50
40
36
100
40'
36'
36''

Figure 1

Automatic Monitoring Station Embodiment – Logical Units

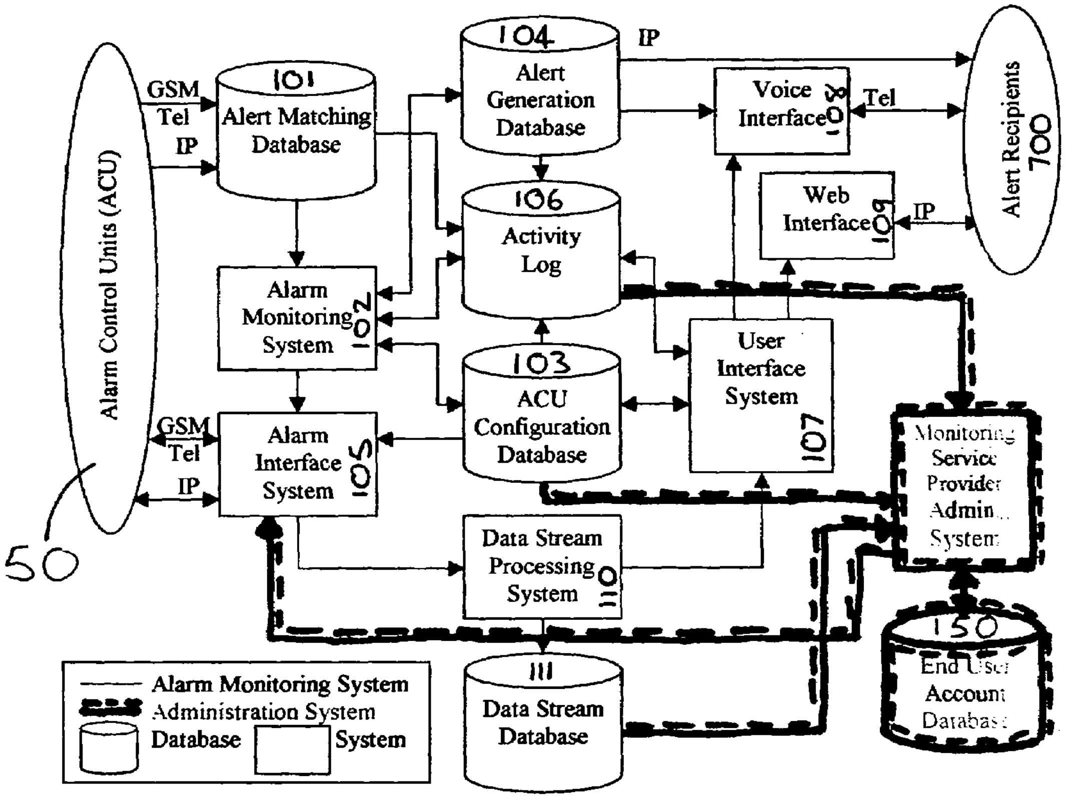

Alarm Control Units (ACU)
50
GSM
Tel
IP
101
Alert Matching Database
104
Alert Generation Database
IP
Voice Interface
108
Tel
Alert Recipients
700
106
Activity Log
Web Interface
109
Alarm Monitoring System
102
103
ACU Configuration Database
User Interface System
107
Alarm Interface System
105
Monitoring Service Provider Admin System
Data Stream Processing System
110
150
End User Account Database
111
Data Stream Database
Alarm Monitoring System
Administration System
Database
System

Figure 2

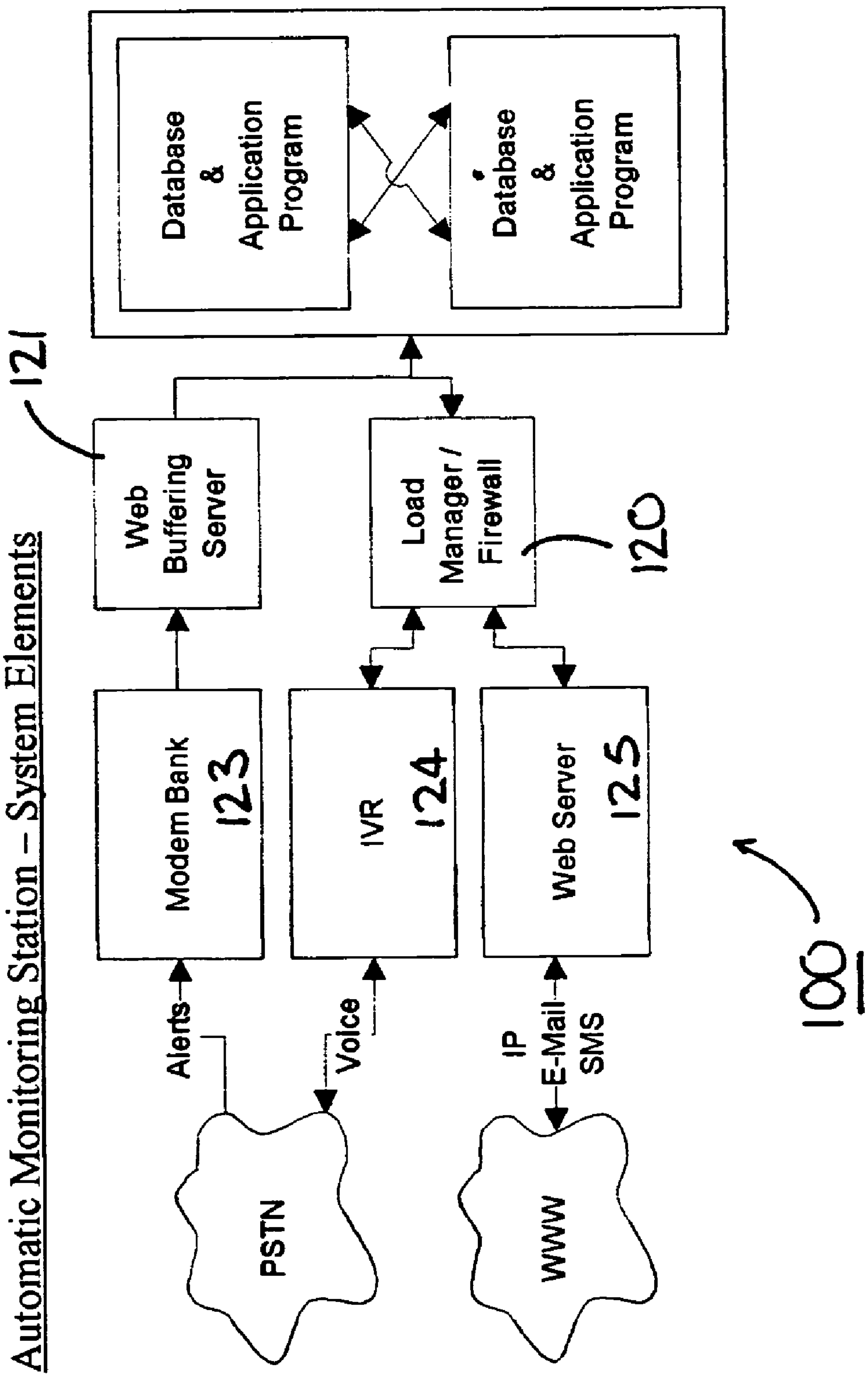

Automatic Monitoring Station – System Elements
PSTN
WWW
Alerts
Voice
IP
E-Mail
SMS
Modem Bank
123
IVR
124
Web Server
125
Web Buffering Server
121
Load Manager / Firewall
120
Database & Application Program
Database & Application Program
100

Figure 3

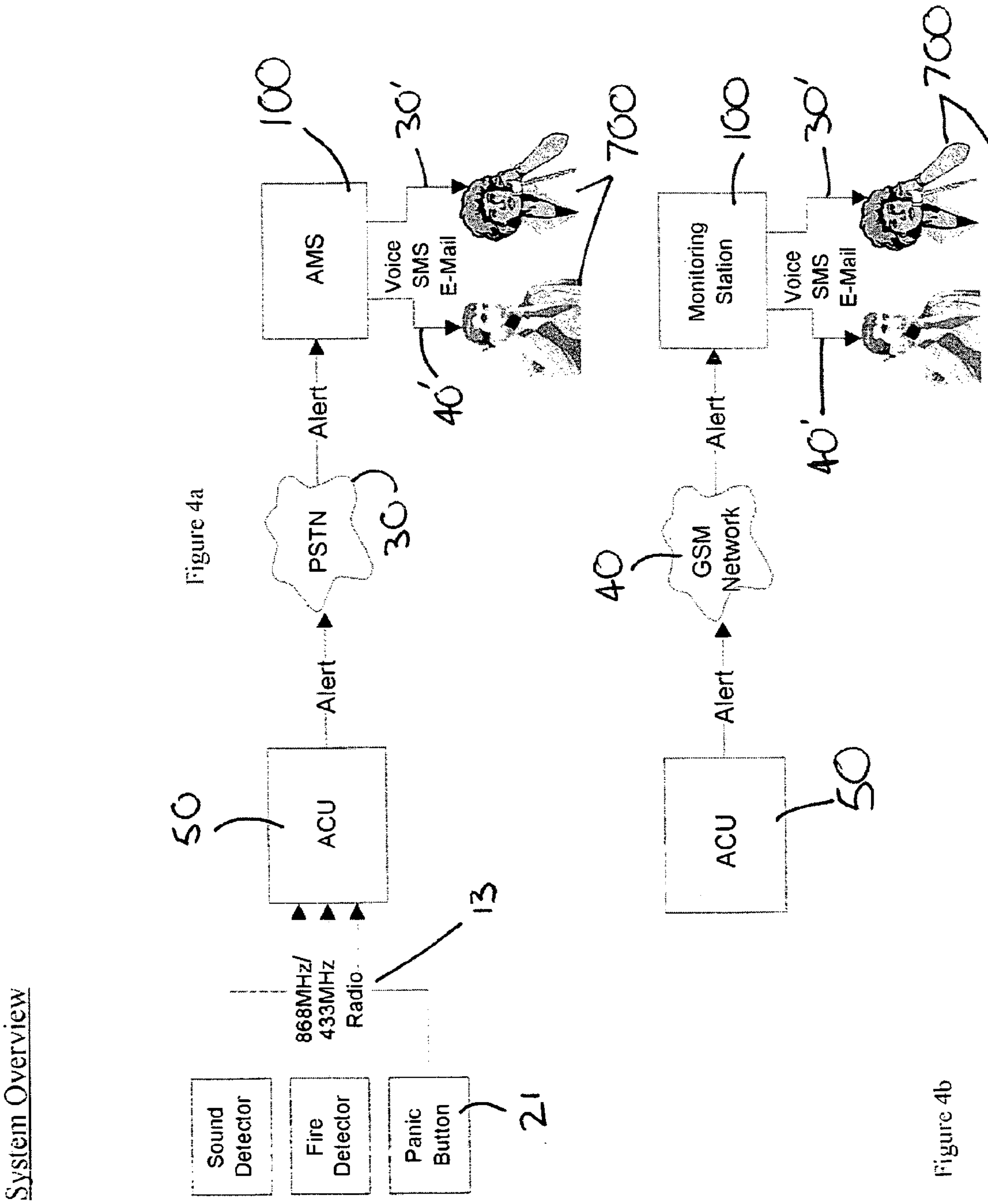

System Overview
Sound Detector
Fire Detector
Panic Button
21
868MHz/433MHz Radio
13
ACU
50
Alert
PSTN
30
Alert
AMS
100
Voice
SMS
E-Mail
30'
40'
700
ACU
50
Alert
GSM Network
40
Alert
Monitoring Station
100
Voice
SMS
E-Mail
30'
40'
700

Figure 4a

Figure 4b

Generated Signals Receiving Unit

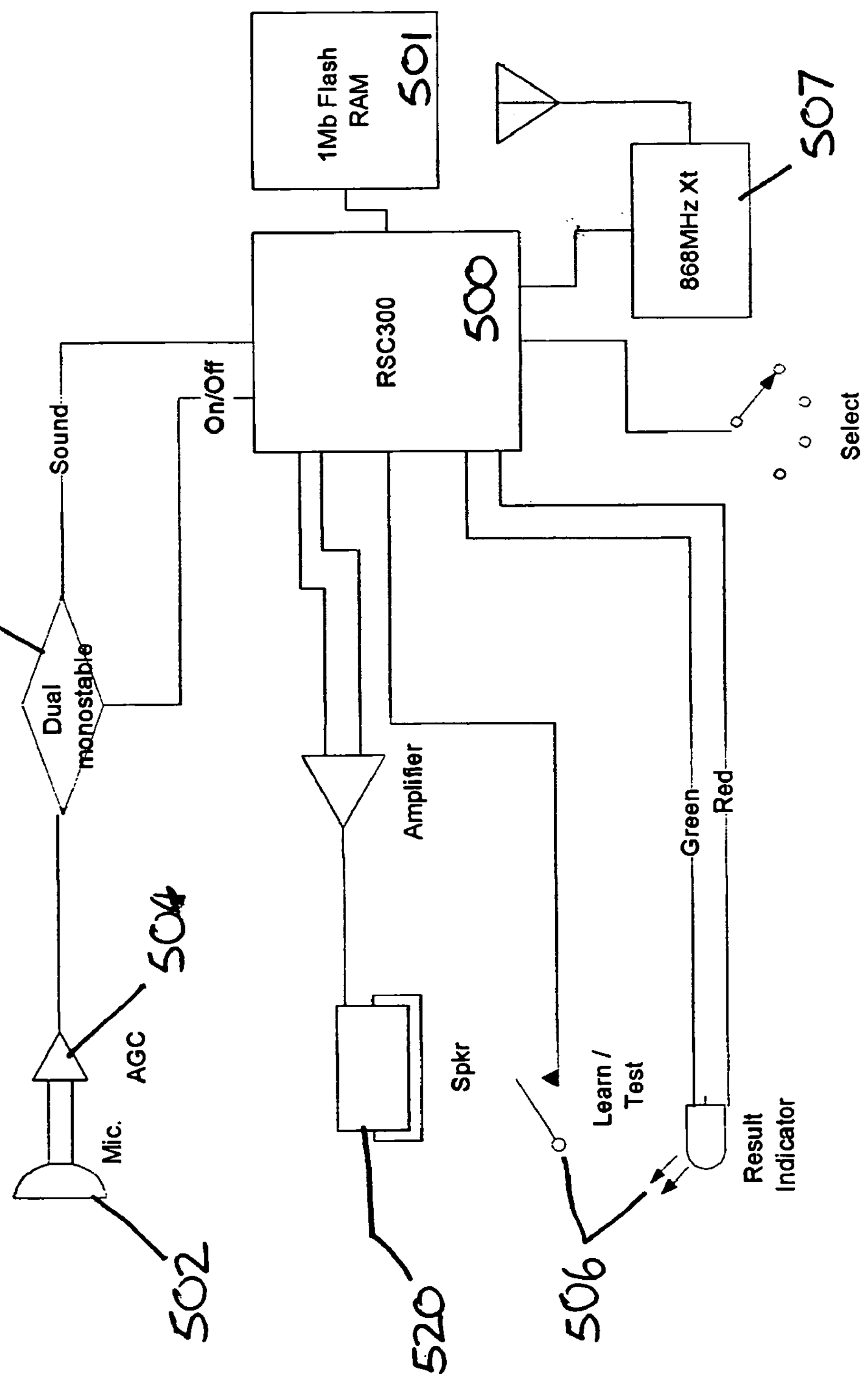

1Mb Flash RAM
501
RSC300
500
868MHz Xt
507
Sound
On/Off
Dual monostable
503
Amplifier
Green
Red
Select
Mic.
AGC
504
502
Spkr
520
Learn / Test
Result Indicator
506

Figure 5

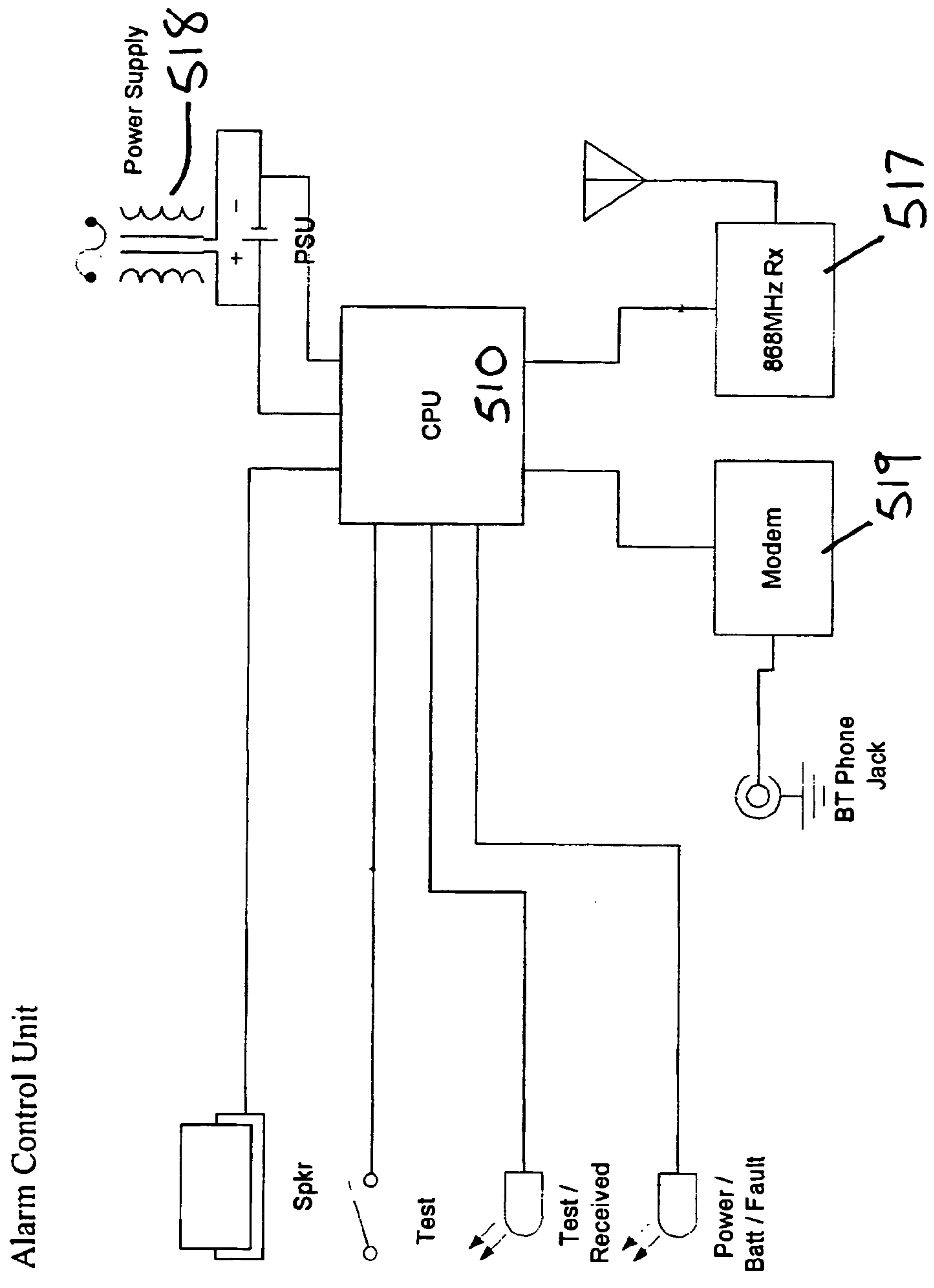

Alarm Control Unit
Power Supply
518
PSU
CPU
510
868MHz Rx
517
Modem
519
BT Phone Jack
Spkr
Test
Test / Received
Power / Batt / Fault

Figure 6

METHOD AND SYSTEM FOR MONITORING EVENTS

TECHNICAL FIELD

The present invention relates to a method and a system for monitoring events and devices and apparatus adapted and configured for use in such a system. More particularly the invention relates to automatically monitoring, detecting and reporting events. Even more particularly the invention relates to automatically monitoring, detecting and reporting breaches of security.

SUMMARY OF THE INVENTION

The invention provides a monitoring and control system comprising: a control unit for receiving signals from a variety of detection devices monitoring events pertaining to security, the control unit having means for transferring information related to the reception of such signals to a remote monitoring station and having control means for actively controlling one or more detection devices; the monitoring station having programmable storage means storing automatic evaluation routines to initiate the automatic transfer of information to a chosen remote user terminal;

wherein the monitoring station is responsive to commands initiated by a remote user terminal, which is remote of the monitoring station and the site being monitored, this may be the chosen remote user terminal or an alternative remote user terminal, to establish a link between the remote user terminal and the control unit to cause the control means thereof to initiate a change in the operative state of at least one of the detection devices.

The invention further provides a method of monitoring a site equipped with one or more detection devices for monitoring events pertaining to security and generating signals in response to detectable events, the method comprising:

utilising a local control unit for receiving signals related to events pertaining to security, the local control unit having means for transferring information related to the reception of such signals to a remote monitoring station and having control means for actively controlling the one or more detection devices;

utilising a monitoring station, remote from the local control unit, to initiate the automatic transfer of information to a chosen remote terminal in accordance with automatic evaluation routines programmed onto the monitoring station; and

enabling the monitoring station to respond to commands initiated from a remote user terminal, which is remote of the monitoring station and the site being monitored and which may be the chosen remote user terminal or an alternative remote user terminal, to establish a link between the remote user terminal and the control unit to cause the control means thereof to initiate a change in the operative state of at least one of the detection devices.

The invention also provides an automatic monitoring station for receiving first information related to events detectable by detection devices, the monitoring station comprising means adapted to receive such first information and programmable storage means storing:

i) routines for evaluating received first information,

ii) a record of actions to be taken in response to a variety of types of evaluated first information,

iii) routines for matching evaluated first information to a particular stored action or set of actions, and

iiii) routines for initiating the matched action or set of actions; wherein some actions include transferring second information relating to detected events to a chosen remote terminal.

The invention also provides a control unit for receiving alarm signals generated by detection devices in response to detectable events, the control unit comprising interface means for receiving generated signals and means for transmitting information relating to the generated signals to a remote monitoring station.

Such a control unit can be suitably utilised as a local control unit or control unit in accordance the method or system of the invention, but may also be provided as a stand alone unit to receive signals and transmit information relating to received signals pertaining to security to transmitted to any remote monitoring station. A particularly useful application of a control unit enables a site with a previously installed non-monitored security system to be monitored. The control unit enables the transfer of information relating to detectable events from the installed security system to a monitoring station by receiving and processing alarm signals generated by detectors in the existing installed system.

In some embodiments of the invention the system comprises a plurality of detectors making up a detector array or network, one or more interface units and a local control unit (Alarm Control Unit, or ACU). These elements are located at the site that is to be monitored, and may be connected by wires or may be in wireless communication. Generally the interface units may be considered part of the local control unit, even if they are physically discrete. The system further comprises a remote monitoring station (which may be an Automatic Monitoring Station, or AMS). An AMS may be capable of communicating with a large number of ACUs, for instance via fixed or mobile telephony.

The AMS can respond to events according to preset commands or routines, which are recorded in a database. The response can include verifying the event and where necessary initiating a transfer of information relating to an event to a chosen remote user terminal. The remote user terminal may conveniently be a PC, a PDA, a mobile phone or WAP enabled mobile phone, or a fixed line telephone. In some embodiments of the invention it may be possible to provide the AMS with transmitted information including verification of the event. The nature of the event and verification may be determined by the ACU or by the detection device intended to respond to that event, although generally it will be desirable to allow the AMS to deal with raw information.

An ACU may provide a common interface for alarm signals generated in response to events detected by the detectors. For instance, the ACU may detect any alarm signal outputs from the detectors and transmit an alert, that is, information relating to such signals, to the AMS. Alternatively the ACU may monitor and log alerts/information relating to such signals, transmitting the information when interrogated by the AMS.

At least some detectors may issue signals of the same general character, for instance they may issue audible alarm signals in response to an event. They may additionally or alternatively issue visible alarm signals, IR alarm signals, RF alarm signals. In one embodiment of the invention the ACU is equipped with means for distinguishing between different signals of the same general character.

In preferred embodiments of the invention the AMS has the ability to instruct the ACU to arm or disarm itself. This has numerous applications, for example:

- The alarm can be deactivated just for the duration of a tradesperson's (or similar) visit, then reactivated, thus avoiding the need to give the tradesperson the PIN code or disabling the alarm for the entire user absence.
- The alarm can be activated if the user has forgotten to activate it before going out, or activated remotely after children or staff or others who may not be entrusted with setting the alarm have left the monitored site.
- The alarm can be deactivated if the user has armed the system in error—for example when a visitor is expected who has means of entry but who does not know how to disarm the alarm.

In other preferred embodiments of the system, the AMS can be utilised to perform zonal monitoring of a site. In zonal monitoring a number of detection devices are used to monitor a site for detectable events. Patterns of signals generated by detectors may be recorded and analysed to determine or verify the nature of an event or security breach. The AMS may be programmed to require a sequence of events to be detected, such as IR detection in different parts of the monitored site within a predetermined time limit, to be detected or require two types of events, such as breaking of electrical contact at one detector and change in ambient temperature at a second detector, to be detected before carrying out a particular action. In other cases the AMS may inhibit transfer of information to a remote terminal or otherwise modify an automatic evaluation routine unless it receives information relating to a second event in addition to information relating to a first event. Such a function is useful to prevent an AMS issuing false alarm calls to a chosen remote user terminal where, for example, a detection device is faulty and repeatedly generates signals then received by an ACU, or, for example, the remote terminal is located at a police station or private security firm whose officers or staff will only attend the site where an security breach can be confirmed. As used in this specification, the term "zonal" does not imply that events must be detected in different parts of a monitored sites, merely that signals from more than one detector can be separately identified.

The method, system, devices and apparatus of the invention may be used to provide a site monitoring service to end users. An end user is able to tailor the service provided by configuring the AMS and/or the ACU. The end user may access the AMS via a remote terminal. Typically, but not exclusively, the remote terminal will be an internet enabled PC, mobile telephone or television. The user will be presented with an user interface allowing him or her to amend, for instance, what events are monitored, when they are monitored, or to where alerts are sent. The user may also be able to reconfigure other elements of the monitoring system, such as detection devices, where this is provided for. In addition the user may be able use the user interface to request supplementary information relevant to an alert, such as live video or audio feeds from further detection devices, to verify the nature or circumstances of the event causing the alert.

The method, system, devices and apparatus of the invention may be used to monitor sites for any event where detection and alarming may be required, particularly hazardous events and examples include fire, flood, intruder alert, alerts for poisonous or hazardous gases or chemicals, and alerts for other events also pertaining to the security of a monitored site. Generally one or more of the following types of detection devices will be utilised:

- PIR intruder detector.
- Carbon monoxide detector.
- Gas detector (natural gas).
- Circuit breaking detector
- Power failure detector (activates if power is interrupted for more than a predetermined length of time).
- Flood detector (activates if water is detected between two electrodes).
- Temperature detector (activates if temperature moves outside precept limits).
- Sound detectors—two types are possible:
  - the first activates if prolonged sound above a certain level is detected (e.g., the bell of a proprietary, fitted, alarm system), and
  - the second activates if certain sudden sound wave patterns are detected (e.g. breaking glass).
- Light detector.
- Voice activated detector for number dialling and voice transmission
- High-resolution real time video utilising compression/decompression software suitable for Internet streaming.

U.S. Pat. No. 5,319,698 discloses a security system comprising sensor units, a receiver for receiving signals from the sensor units, a transmitter activated by the receiver, which transmits a signal to a local security station and activates an alarm and a sequence of telephone calls. This system has the disadvantage that the user cannot alter the operational status of the system remote from the monitored area.

BRIEF DESCRIPTION OF THE FIGURES

Other aspects and features of the invention will be apparent from the following description in which embodiments of the invention will be described, by way of example only, with reference to the figures of the accompanying drawings. In the drawings:

FIG. **1** illustrates schematically the elements of a system constructed in accordance with the invention.

FIG. **2** illustrates schematically the logical units of an automatic monitoring station constructed in accordance with the invention.

FIG. **3** illustrates schematically the elements of the automatic monitoring station constructed in accordance with the invention.

FIGS. **4***a* and **4***b* illustrate schematically the way in which the system can be used to send an alert.

FIGS. **5** and **6** illustrate schematically elements of a local control unit usable in the system and constructed in accordance with the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

To aid interpretation of the description of examples of the system and apparatus of the invention, and methods of monitoring sites, using the system and apparatus, of the invention a glossary of some terms used is provided:

ACU	An Alarm Control Unit. This is a local control unit provided at a monitored site. The ACU is adapted to receive signals generated in response to events by detection devices also located at the monitored site, process the signals and transmit information relating to the received signals to a remote monitoring station
AMS	An Automatic Monitoring Station. This has programmable storage means allowing it to identify events pertaining to security detected by detection devices and carry out actions determined by the nature of the identified event. Some of the actions will include automatically sending information pertaining to security to a chosen remote terminal. In some embodiments of the invention, a user of a monitoring system utilising the AMS may alter the actions or sequence of actions to be taken by instructing it from a remote terminal.
Alert	A signal from the ACU to the AMS indicating that a detector has been activated. The message may include the detector identity, type and information describing the nature of the alert.
Alert Actions	The actions that the system user has instructed the system to undertake in response to a particular type of Alert.
Alert Recipient	A person or device chosen to receive a message from the AMS following an Alert.
Arm	The ACU is armed by various means, including entering a code via a keypad of using a radio-signalling device or a key, or receiving a message from the AMS to arm. When the ACU becomes Armed the ACU may wait for a pre-determined period (typically less than one minute) after which any Detectors signalling to the ACU that they have detected an event are assumed to be valid. The ACU may inform the AMS that it has been armed.
Cancellation Message	A message sent from the ACU to the AMS informing the AMS that a valid Cancellation Sequence has been received in respect of a particular Provisional Alert.
Cancellation Sequence	A mechanism (such as the entry of a PIN Code into a device connected by wires or wireless to the ACU) by which the customer can inform the ACU that the recent Detectable Event is not to generate an Alert. The Cancellation Sequence must be correctly carried out within a short period of the Detectable Event. If it is not an Alert will normally be generated.
Detectable Event	Anything that causes a detector to be activated and that would, in the absence of a correct Cancellation Sequence, cause an Alert to be generated.
Disarm	The ACU is disarmed by various means similar to those used to arm it. When the ACU becomes disarmed is sends a message to any Detectors capable of acting upon the message and so configured that they ACU is disarmed and that the Detector may also disarm itself. Some detectors (for example those monitoring smoke, dangerous gasses and activation of a panic or personal attack button) are never disarmed and the ACU always remains Armed in respect of such detectors. The ACU may inform the AMS that it has been disarmed.
PIN Code	A secret customer-specified sequence of number (or letters or other type of code) used to arm and disarm the ACU.
Provisional Alert	A message sent from the ACU to the AMS informing the AMS that a detectable event has occurred and for which there remains an opportunity for a valid Cancellation Sequence to be generated.

With reference particular reference to FIG. **2**, an AMS (**100**) may contain the following logical elements:

Alert Matching Database (AMD) (**101**)

The AMD (**101**) consists of a database, a telephony interface and an IP interface to receive Alerts from any ACU (**50**). The AMD receives messages from the ACU and may also detect Calling Line Identification (CLI), which may be used to authenticate the message.

When the AMD receives an Alert from an ACU, which may happen every time an armed ACU is activated, the Alert is stored in the database together with the time of receipt. When a Disarm message is received the AMD will identify any corresponding Alert which may be in the database and the Alert/Disarm sequence will be logged in the Activity Log and no further action will be taken. Any Alerts which are not followed within a given period by a Disarm message will be treated as Alarms and are sent to the Alarm Monitoring System (AMSys) (**102**) for processing. In the case of a Panic Alert this creates an immediate alert without the buffering and disarm time lapse described above.

The following truth table describes the action of the system when matching Alert and Disarm codes are received with the same ACU identifier, but different CLI is received to that expected.

	Order of Verification →		
	CLI Does Not Match ACU Verification Table	CLI Missing	CLI of Disarm Does Not Match CLI of Alert
Alert Message	Generate 'Have you changed your phone number' letter. Otherwise normal operation.	Normal operation.	N/A
Disarm Message	Normal operation.	Instruct AMS to request PIN Authentication. If this fails reject Disarm Message.	Reject Disarm message. Generate additional Action Log entry 'Disarm Tamper Detected'

In other embodiments CLI is not used, but the identity of the ACU is transmitted as part of the message from the ACU to the AMS

Logically, the AMD may consists of two principal tables:

1. Active Alerts Table. Stores Alerts, Alarm Unique Identifier and Associated Calling Line Identification which are less than a given period old and against which Disarm messages have not been received.
2. ACU Verification Table. Matches Alarm Unique Identifier with Calling Line Identification.

Alarm Monitoring System (AMSys) (**102**)

This is the intelligence embedded within AMS (**100**). When an Alert is passed on from the AMD (**101**) the AMSys (**102**) consults the ACU Configuration Database (**103**) to decide what action to take. AMSys (**102**) has priority access to the ACU Configuration Database (**103**). Having determined the appropriate action to take the AMSys makes an entry into the Activity Log (**106**) and instructs other systems to carry out actions. Possible actions include:

Request PIN Authentication. The Alarm Interface System (AIS) (**105**) phones the monitored site to request a PIN entry via a telephone handset. The recipient is given, say, three attempts or 1 minute to enter the correct PIN. If no correct PIN is entered then the Alert is treated as genuine, subject to alarm verification and the ACU (**50**) is instructed to sound local sirens (**20**) if applicable.

Determine the nature of the alert.

Send messages (voice, IP, SMS or Pager) to specified Alert Recipients.

Make entry in Alert Action Log.

Record and analyse Zoned Activation for alert verification system.

Instruct Data Stream Processing System (**110**) to open a channel to the ACU (**50**) for download of sound or video, or instruct Data Stream Processing System (**110**) to manage transfer of sound or video from ACU for storage and possible onward transmission.

Send an e-mail message

ACU Con figuration Database (ACUCD) (**103**)

The ACUCD (**103**) may contain:

System Configuration Table (SCT). A description of the current configuration of the Alarm System (identical to that stored locally in the SCT) and current alarm status, including any zones activated.

Alert Action Table. List of actions to be taken when a particular Alert is detected.

Alert Generation Database (AGD) (**104**)

This database oversees the transmission of messages to Alert Recipients (**700**) if no disarm has taken place. The AMS (**100**) may, in response to an Alert, identify that various Alert Recipients (**700**) need to be informed and the address where the alert has been activated. These recipients and the associated location and alert identifying message is passed to the AGD (**104**) that manages the transmission of those messages (i.e. queues, repeat attempts and so on). The AGD (**104**) interfaces to the Voice Interface (**108**) for messages using voice synthesis. For IP based messages the AGD has a direct Internet connection (**30"**).

All Alerts, Message attempts and their result are recorded in the Activity Log (**106**). For example, there may be entries made containing information similar to the below, presented in a manner similar to the below:

Date and Time	Message	Alert Recipient	Result
15/11/00 12:19 AM	Intruder Alarm Alert Received by MyGard	N/A	N/A
15/11/00 12:20 AM	Intruder Alarm Alert phone call to Mr J. Bloggs	(07790 926039)	No Answer
15/11/00 12:20 AM	Intruder Alarm Alert pager message to Mr F. Brown	(0207 926 0394)	Sent
15/11/00 12:25 AM	Retry: Intruder Alarm alert call to Mr J. Bloggs	(07790 926039)	Answered
15/11/00 12.25 AM	Intruder Alarm activated at (address) Abel Security	e-mail address	Acknowledged

The AGD will also manage communications with Police Control Rooms, private security response units and the Fire Brigade. The AGD will generally deal with jobs in First In, First Out (FIFO) order, except for Panic Alerts that receive immediate attention. Keyholders who, if police/private security are attending, will be contacted early in the alert cycle and asked to confirm their attendance automatically by pressing the * button on their phone—this action is then registered on the Action Log

Alarm Interface System (AIS) (**105**)

The AIS (**105**) is used for general two-way communication with the user's ACU (**50**) but not Alert messages and Disarm messages, which are sent to Alert Matching Database (**101**). It is intelligent in that it can undertake complex tasks, such as uploading a revised SCT and updating the ACUCD (**103**) or managing a video stream from an ACU. Generally, the AIS (**105**) is separated from the AMD (**101**) because the former deals with time critical activities only (receiving Alerts and Disarms) whilst the AIS deals with a more complex range of interactions.

Generally, the AIS (**105**) is fault tolerant and is able to prioritise its resource utilisation based on the importance of the activity. The AIS will keep track of its resource utilisation and could use a negative acknowledgement such as 'Try Later' or similar to non-time critical requests from ACU's if resources are scarce.

AIS can undertake housekeeping tasks, such as changes to system configuration or resetting after an Alert, send remote instructions to the ACU, such as remote arm and disarm, and activate data stream devices and receive inbound signals, for instance sound and video, and pass these to the data stream processing system for analysis.

Activity Log (**106**)

This records all events that are of relevance to a user. The Activity Log (**106**) conveniently serves at least these functions:

- It provides feedback to the user as to the status of the ACU (**50**) and the source of any alarms that may have been activated, and the Alert Recipients (**700**) contracted.
- It allows the user to use the monitoring system as a personnel-monitoring tool (e.g. to check whether contract security patrols have taken place or personnel have arrived at work on time). A simple filtering tool may usefully be provided to allow the user to focus on useful messages only.

User Interface System (UIS) (**107**)

This system links the web interface (**109**) and/or the voice interface (**108**), described hereinbelow, to those databases which supply information available to the user. The UIS (**107**) manages firewalls and password protection to prevent unauthorised access to Alarm Configurations.

Users are able to change Alarm Configurations via the web; these changes are delayed for a period of time so that a message can be sent to the previous Primary Contact to inform the user that a change to the Alarm Configuration is about to be enacted. Thus if an intruder attempts to disable an alarm by gaining unauthorised access to the web site, they will be detected by the user. However, initial configuration need not be delayed.

Another security feature of monitoring system is that user identification details, for instance PIN, name, address, primary (e.g. home) telephone numbers, are held in the

User Account Database (**150**), which cannot be queried by the UIS (**107**). Thus any unauthorised user who evades the password security and manages to access and Alarm configuration will not easily be able to identify the protected monitored site.

Voice Interface (**108**)

This is based on a voice recognition system that may be configured to perform two tasks:

It delivers synthesised voice messages for outbound alert messages to alert recipients (**700**).

It permits inbound callers to check their alarm status by synthesised voice response. The system will, after entry of correct identification, relay the current alarm system status and then read out the contents of the Activity Log (**106**). This would generally be reported as the most recent alarms first, followed by actions taken.

Web Interface (**109**)

This interface (**109**) can be developed so that it is suitable for accessing from a variety of remote user terminals. For example it may be accessed via terminals enabled for using the WWW, WAP or interactive digital television (iDTV).

The User Web Interface (**109**) usefully permits users to carry out two basic tasks:

- Check current alarm status and send remote arm/disarm messages.
- Set or change the response to particular Alerts.

In some embodiments it may also permit users to set or change the configuration of the Alarm Unit.

Remote Arm/Disarm enables a user to arm and disarm the ACU (**50**) via the Web. This allows a user to allow entry to the monitored site (e.g. by tradespeople) without having to leave the monitored site unprotected all-day or giving the PIN to tradespeople. It may also allow remotely controlling, for instance via a mobile phone or other connectable device, other door locking and unlocking.

Remote Disarm messages are always copied to the Primary Contact to detect unauthorised disarm attempts. Users can elect to allow or disallow Remote Disarm. Users can subsequently change their election, requesting such a change via the web or other means. Activation of Remote Disarm is delayed for a period of time and the Primary Contact is notified of the request by post and voice or messaging.

User Account Database (**150**)

This maintains information about the user (name, address, and primary contact number) which is physically inaccessible to the UIS (**107**).

Automatic Data Stream Processing System (DSPS) (**110**)

Streamed data (sound and compressed video) from an ACU (**50**) can be directed to the DSPS (**110**) by the AIS (**105**). The DSPS (**110**) may have a range of analysis tools to analyse the signal:

- Immediately after an alert activation it could compare a variable sound feed to a sample ambient noise level to determine intruder activity.
- Immediately after an alert activation it could compare the data bits and edges and surfaces of two or more video images to detect sudden changes in the image (other than light intensity).
- Immediately after an alert it could pass sound or video to an IP address for remote monitoring.

Alternatively, the ACU (**50**) may have verification software embedded within its functionality which can perform the tasks described above, obviating the need for a separate DSPS (**110**). In such embodiments the ACU may also be configured to perform zonal monitoring as described hereinbelow. The ACU would then send a verified alert signal to the AMS to instigate a pre-set response by the relevant AMS database.

Data Stream Database (**111**)

This stores reference images and ambient noise levels for comparison purposes, and also stores inbound images for future retrieval, for instance a still picture triggered by a movement detector activation.

These logical units will generally be located together in one physical part of the AMS (**100**). FIG. **3** illustrates how the AMS can have access to the databases and application programs controlled by a firewall (**120**) and web buffering server (**121**). The firewall and web buffering server are located between the hardware storing the databases and application programs and the means for connecting to the ACU and users and Alert recipients. Connection may be made through a public switching telephone network (PSTN) (**30**, **30'**, **30"**) or GSM network (**40**, **40'**). A modem bank (**123**), Interactive Voice Response System (IVR) (**124**) or web server (**125**) allow such connection to be made.

Web buffering is a further security mechanism present in some embodiments for preventing intruders from disabling the ACU before an alert message has been sent.

Where Web Buffering is enabled the ACU will send a Provisional Alert to the AMS immediately whenever a detectable event occurs, without waiting for Cancellation Sequence. If a Cancellation Sequence is subsequently received by the ACU then a Cancellation Message is sent to the AMS. If the AMS receives no Cancellation Message within a specified time then the AMS will commence execution of the relevant pre-set Alert Actions.

Using this further security method, a Provisional Alert will be generated very quickly following a Detectable Event, thereby greatly reducing the opportunity for an intruder to disable the ACU by, for example, destroying it. Furthermore, the availability of such a mechanism increases the risk associated with attacking any ACU, as the intruder will not know whether Web Buffering has been enabled and therefore cannot predict whether an attempt to disable the ACU will be successful.

The UIS can enable a user to reconfigure the parts of the system located at the monitored site by relaying instructions to the ACU, and in some cases the detection devices, through the AMS.

Remote Configuration of the ACU

The User AMS Interface can be used to allow the user to change the configuration of the ACU (for example, changing the sensitivity of a detector, or the time permitted to enter a Cancellation Sequence.) This permits a more flexible and comprehensive user interface to be developed for the ACU than normally the case with alternative home or business monitoring and/or security products.

Remote Maintenance and Upgrade of the ACU

The ACU may be reprogrammed remotely by the AMS, by means of messages sent by the AMS to the ACU, which is stored in non-volatile memory. The AMS uses this memory to carry out appropriate actions when the software originally supplied with the system suggests no appropriate actions.

EXAMPLE 1

A new type of detector may be introduced into the detector network that requires the ACU to carry out a specific sequence of actions in response to detected events. A fresh instruction code can be transmitted from the AMS to the ACU, and stored thereon, as a programme module.

The AMS can also ensure that the AMSys Configuration record is consistent with the ACU configuration by remote reprogramming.

Transmission of Messages from the AMS to the ACU

Other communications may be passed between the AMS and ACU. Where the AMS is adapted to transmit messages and data to the ACU:

Text messages can be transmitted to the ACU for display on the screen, which would be immediately visible to the first person entering the monitored site.

A temporary PIN code can be sent to the ACU to permit a visitor to a monitored site to arm or disarm the system a single time without revealing the normal user PIN code.

Messages can be used to allow remote triggering of a variety of devices in the monitored site. Examples include remotely unlocking a door, programming a video recorder, controlling central heating and so on.

Reconfiguring the System via the User AMS Interface (**107**, **108**, **109**)

This interface (**107**), accessible via the Internet, portable communications devices such as WAP phones, and voice telephony, allows the user to instruct the AMS (**100**). Suitable security must be built into the AMS to prevent unauthorised access, which could permit the alarm to be disabled. Measures include:

Use of encrypted passwords and memorable data.

Use of a device-generated time-dependent code sequence.

Incorporation of feedback to the last known user contact point confirming the instructions received through the User AMS Interface (**107**) (thus allowing the user to detect unauthorised access.)

Incorporation of a time delay in carrying out instructions that might compromise the effectiveness of the system (such as changes to Alert Actions, remote configuration commands and the like.)

Ability to Perform Actions Specified by the User in Response to an Alert

Users are able to use the User AMS interface (**107**) to record the actions they would like to take place when specific Alerts occur. These actions would form the basis of the pre-set routines stored on the AMS that enables the AMS to respond to events. A wide range of Alert Actions may include:

- Initiation of an Automatic False-Alarm Reduction Check
- Recording of the Alert in the Alert log.
- Automatic placement of telephone calls to Alert Recipients (**700**) by means of Voice Synthesis software, informing the Alert recipient of the Alert.
- Automatic generation of an e-mail to an Alert Recipient informing the Alert recipient of the Alert.
- Automatic generation of a message to a pager or other mobile device informing the Alert recipient of the Alert.
- Automatic recording of the Alert and subsequent Alert Actions in the Activity log (including failed attempts to carry out an Alert Action.)
- Specification of times of the day, days of the week and holiday periods when the Alert Action should not be carried out, for example to not call elderly relative after 10 PM to inform them of mains power failure or other minor events.
- Automatic notification of Alert to police, private security firm, fire brigade or other nominated party.
- Automatic triggering of a call to pre-determined User number, such as a mobile phone number, to ask a user whether they would like attendance by private security firm.
- Automatic initiation of video image capture or sound recording.

The Alert Recipient may be, but not essentially be, the user. The user may also nominate further Alert Recipients or nominate different recipients for Alerts relating to different events. Any number of Alert Actions can be associated with an Alert. If the AMS is unable to complete an Alert Action it should continue to attempt to complete the action for a finite period, or until the Alert is cancelled.

If an Alert is cancelled following a Cancellation Sequence the AMS can be configured to contact all Alert Recipients with a message that the Alert has been cancelled and no further action is required.

Visual Presentation of Activity Log

Users may view the Activity Log (**106**) via the Internet, or by dialling in to an Interactive Voice Response System, described hereinabove, that can read out the contents of the Activity Log using voice synthesis software.

The Activity Log (**106**) conveniently provides three functions:

1. It can be used to test the system. When the system is in 'Test' mode Alerts are generated as normal and logged in

the Activity Log, but no other Alert Actions are carried out. Thus, a user can activate all the detectors in the system and verify that Alerts are generated.

2. It can be used to check the response to an Alert. This has two main benefits in use:
   a) The user can determine which Alert Actions were carried out and take steps to cancel any actions on the part of the recipients if they are not required, e.g. if there is a false alarm, and
   b) Verify that the AMS carried out the correct sequence of actions in response to an alert, e.g. if an Alert Recipient did not receive a message the Activity Log may reveal that call attempts were made but the phone line was engaged.
3. It can be used to provide a monitoring function. The monitoring may be required by a business that wants to verify that security staff do, in fact, make periodic patrols within an office. A monitoring system equipped with a movement detector could record the Alerts generated by the security staff for service verification purposes, but take no other action.)

Some embodiments of the system can be provided with further preferred features:

Visual Display of Remote Video Images or Remote Sound

In an ACU equipped with circuitry enabling a video image detector, video information may be sent directly to the AMS in response to an instruction from the AMS to so do.

These video transmissions might take advantage of video compression technology inserted between the video capture device and the ACU, and decompression software and hardware within the AMS.

The AMS is able to record these images on computer storage devices and, in response to an instruction from the user via the AMS user interface, relay the images on via the internet or other telephony link for viewing by the user or by third parties such as the police. The AMS is also able to archive these pictures for later evidential use.

The foregoing may also apply where a sound detector rather than a video image detector is included in the network of detectors.

Automatic False-Alarm Reduction Check

The user may choose to have the AMS perform an Automatic False-Alarm Reduction Check upon receiving an Alert and prior to undertaking any other Alert Actions.

The Automatic False-Alarm Reduction check involves the AMS calling the monitored site where the alarm is located, or the user via a mobile communications device, and requesting a PIN number, or some other code or unique identifier. The user may be asked to provide the code by means of a synthesised voice generated by the AMS, or through other means, such as text messages. If the user correctly enters the code then the Alert is considered to have been activated by mistake. If the correct response is not received then the AMS continues to carry out all the Alert Actions associated with the Alert.

The Automatic False-Alarm Reduction Check may be enabled or disabled by the user via the User AMS Interface.

Zonal Monitoring at the AMS

The AMS contains a description of the configuration of each alarm system it is monitoring, and it maintains a database of alerts received from the local ACU. It is therefore possible to offer a zonal monitoring system that detects successive alerts from the same ACU to detect multiple indications from different detectors within the same monitored site.

The AMS can be configured to generate its own zonal alerts, which can have a set of associated alert actions in much the same way as ACU generated alerts. This will allow AMS to offer a zonal detection system that will greatly reduce false alarms due to erroneous detection.

EXAMPLE 2

A house is fitted with three movement detectors and two contact switches. The owner does not want external sirens to be activated or police to be called unless two or more detectors are triggered, and has created a zonal alert within the AMS to this effect.

An intruder breaks in and activates a movement detector. The ACU uses web buffering to inform the AMS and requests a Cancellation Sequence, which the intruder is unable to supply. AMS registers the alert and carries out Alert Actions associated with the detector. The intruder moves around the monitored site and activates a contact switch, which generates a second alert. The ACU immediately activates local sirens and informs the AMS, which recognises that a second detector has been activated and generates a zonal alert. The associated Alert Actions for the zonal alert are carried out, which Alert Actions may include notification to police.

In this way the AMS is able to perform zonal monitoring for many ACUs. This reduces the chances of triggering responses to false alarms caused be erroneous detector activation.

Activation of Sound Feeds as an Alert Verification

The AMS can instruct the ACU to activate a microphone and transmit a continuous sound feed from the microphone through the ACU to the AMS. The AMS can monitor this sound feed for unexpected sounds that may indicate the presence of an intruder. This could be used to provide additional verification of an intruder to police.

AMS can also relay the sound in real time to a user (or other specified recipient) via the Internet, allowing the user to listen to sounds within the monitored site. The sound detection could be used to detect other audible events, such as an audible alarm or, where monitoring is provided at agricultural sites, sounds indicating that animals may require assistance.

Activation of the sound feed can be an Alert Action in response to an Alert.

Activation of Video Feeds as a Possible Response

The AMS can instruct the ACU to activate a camera and transmit a video feed from the camera through the ACU to the AMS. This video feed could be single frame, low speed or high speed video, could be real time or buffered and could be of various resolutions, depending on the equipment connected to the ACU and the bandwidth available to communicate between the ACU and the AMS. The AMS can perform a number of actions in response:

- The AMS can store images in secure long-term storage for possible later use as evidence of e.g. a security breach.
- By using image-scanning software the AMS can compare a reference image which was captured when the security system was armed with an image taken if the camera is triggered by movement. By detecting significant data variation, which may correspond to the presence of an intruder, this could be used to provide additional verification of an intruder.
- The AMS could receive infrared images to detect the presence of a heat source, which might be an intruder or a fire or a process failure.
- The AMS could relay the image to a user or other specified recipient via the Internet, allowing the user to view the interior of the monitored site, or to view-

stored images. The images can be used to assess the need to respond to a detected event, such as flood, vandalism or security breach.

Activation of the video feed can be an Alert Action in response to an Alert.

EXAMPLE 3

A domestic dwelling has a doorbell that act as a detection device for in the monitoring system and can communicate with the ACU The dwelling also possesses a fixed frame digital camera that takes a picture of the door when the bell is pressed. When the doorbell is rung and the system is armed an alert is sent to AMS. The associated Alert Action is for AMS to instruct ACU to relay the latest picture taken by the camera, allowing the user to remotely verify the identity of the caller. If the user so wishes they could use the other facilities of the monitoring system to remotely disarm the system and unlock the door to permit access.

EXAMPLE 4

A police force requires visual verification of an intruder before it will respond to an alarm. A business premises is equipped with a movement detector, a light and a digital video camera. When movement is detected and the system is alarmed the AMS instructs the ACU to switch on the light and transmit images from the video camera. These are stored at the AMS. The AMS also informs the user of the movement alert. The user may then log on to the AMS via the Internet and view images from the monitored site. If an intruder can be identified then police can be informed of a verified alert.

In alternative examples the AMS could be instructed to automatically compare the image received with a reference image from the same camera and to infer the presence of an intruder if significant differences exist between the observed and reference images.

Ability of AMS to Send Instructions to ACU, Including Operation of Remote Devices Such as Automatic Door Locks

AMS can transmit instructions to ACU that can be relayed to detectors if they are capable of carrying out actions. This can include instructing a camera to take a picture, operating an automatic lock, switching a piece of electrical equipment on or off or controlling other predetermined processes such as controlling of on-off timers in a heating system.

EXAMPLE 5

A pub cellar is prone to flooding. A monitoring system is installed primarily as an intruder detection system, but is also equipped with a water detector and a remote relay, which permits the ACU to switch on or off a normal 240V mains socket. When water is detected in the cellar an alert is generated. An associated Alert Action is that the AMS instructs the ACU to switch on the 240V mains socket. A water pump is connected to this socket and the cellar is pumped dry. A second alert action is that the switch is turned off thirty minutes after it is turned on. If the cellar is still flooded then subsequent water Alert will be generated and the pump activated for a further thirty minutes.

A specific embodiment of the system comprises the following elements:

A plurality of detectors

An ACU adapted to detect alarm signals generated in response to detected events by the detectors

The AMS

The ACU can comprise physically discrete units able to communicate with each other via a local radio link or a fixed, or wireline, link. Generally the discrete units will be a first unit adapted to transmit information relating to generated signals to the AMS and one or more second units adapted to receive generated signals and transmit them, or information relating to them, to the first unit. This allows the generated alarm signal outputs of a number of detection devices to be monitored by a 'single' ACU. Such an arrangement is particularly useful where some of the detection devices generate visible alarm signal outputs in response to detected events, each requiring an uninterrupted line of sight path between the generated signal output and the part of the ACU adapted to receive detection device generated alarm signals. It also allows further detection devices to be introduced into a network of detection devices after the ACU has been set up, merely by placing corresponding further second units in positions where they can receive any signal generated by the further detection devices.

As illustrated in FIG. **5**, the ACU (**50**) comprises an RSC300 chip (**500**), Flash (non-volatile) memory (**501**), a microphone (**502**) with a dual monostable (**503**) to control its operation and an automatic gain control (**504**), a speaker (**520**), user interface controls (such as buttons, lights and switches) (**506**), a low power radio transmitter (**507**), a power supply (which may be a battery, solar powered, mains supplied, or a combination thereof) and other components (resistors, capacitors, logic elements and the like).

As illustrated in FIG. **6**, the ACU (**50**) further comprises an 868 MHz low power radio receiver (**517**), microprocessor (**510**), some non-volatile memory, a power supply (**518**) with battery backup and a modem (**519**).

The software controlling the RSC300 (**500**), and the reference sounds and other data, are stored in the flash memory (**501**). In this way data and the controlling program are preserved in the event of power being lost (such as during the replacement of batteries. Other forms of non-volatile storage can be used in different embodiments, and backup batteries can be used in yet further embodiments allowing volatile memory to be used.

The dual monostable (**503**) is used as a means of switching the microphone (**502**) on for a short period and then off again in response to a signal from the processor. This allows the RSC processor to more reliably interpret sounds. The RSC300 (**500**) is designed to recognise words, and the silence at the start and end of the word are significant. The RSC300's pattern recognition algorithm cannot be interrupted so an external means is required to artificially break down the continuous sound of a siren in to a sound resembling a word, with silences before and after. This can be achieved in one embodiment by means of an electronic timing switch, which is activated by a signal from the RSC300 prior to pattern recognition. The effect of this switch is to disable the microphone (**502**) for a short period (e.g. 0.5 seconds), then enable it for a short period (e.g. 1.5 seconds), and then disable it for a short period again. Thus, the continuous siren tone is reduced to a 1.5 second sound burst. The timing switch instead of being a monostable may be an electronic timer, counter, or some other form of electronic counting circuit capable, upon receipt of a trigger, of disabling then enabling then disabling the microphone.

The RSC300 chip is able to record reference words and then subsequently recognise these words when spoken by the same person. In this invention the chip is used to record the sound of an alarm sounding. Then, when a loud sound is detected, the chip compares this sound with the recorded sound of the alarm sounding. If the two sounds match then the generated signal receiving unit sends a signal to the part of the ACU adapted to transmit information relating to the generated signals to the AMS, using the low power radio transmitter (**507**).

The signal receiving unit may be taught a number of reference sounds, in which case the message sent to that part of the ACU (**50**) adapted to transmit information relating to generated alarm signals to the AMS (**100**) can indicate the particular sound that was detected. In this way the ACU can recognise, and distinguish between, different alarms.

One problem with this approach is that occasionally the generated signal receiving unit may generate a 'false positive' signal when it mistakes a non-alarm sound for an alarm signal. Three methods may be used to reduce the likelihood of these false positive situations:

1. The automatic gain control has a user-selectable sensitivity allowing the system to respond only to sounds above a predetermined threshold (such as sirens and alarms) and to ignore normal background noises such as children's toys.
2. The software driving the detector incorporates an algorithm that initially requires a high degree of correlation between the observed sound. If a match is not found then subsequent samples and matching attempts are made until two (or more) matches against the same reference sound are obtained. The degree of correlation required can be allowed to fall as the number of samples increases. This method is useful if there is a possibility of one alarm sound being mistaken for another, or if a sudden and loud noise (such as something being dropped) generates a random pattern. In both cases the algorithm described will reduce the chance of a false positive result.
3. The generated signal receiving unit can have the ability to be taught other noises which it should ignore. So if, for example, a particular toy generates a sound which might be mistaken for an alarm then by recording the sound of the toy and checking for a pattern match against both the alarm sound and the toy sound the unit will match best against the toy, even though the match against the alarm would otherwise be adequate. Thus, false positives can be reduced to a low level.

Other means of reducing the impact of false-positive alerts can be built in to the AMS, by having the AMS place a check call to the monitored site. It is unlikely that a sound, that could be mistaken for an alarm, would occur within a monitored site when that monitored site are unoccupied.

EXAMPLE 6

The generated alarm signal receiving unit is trained to recognise three distinct alarm sounds: the 'Door Entry Alarm' which is heard when an authorised entry route is used to enter a monitored site with a an activated alarm, the 'Intruder Alarm', which sounds when an intruder is detected, and a 'Smoke Alarm', which can be completely independent of the intruder alarm system. The unit is also trained to recognise two 'Reject' noises—a vacuum cleaner and a child's toy.

In this embodiment the RSC300 is normally in 'sleep' mode, to reduce power consumption. When a sufficiently loud noise is detected an interrupt is generated which awakens the RSC300. The software controlling the RSC300 then takes repeated samples from the microphone and matches this sound against the recorded reference sounds. If the best match is not sufficiently good to be classified as a valid result then the recognition strictness is reduced and further readings are taken. If the best match is good enough to be registered as valid then the match is noted and further readings are taken. Once a maximum number of readings have been made, or two readings have yielded the same result, the software stops taking further readings and proceeds as follows:

If the same reference sound has been matched twice then the sound identification is confirmed and the sound identity is the matched reference sound. If one or more sounds have been matched only once then the identification is unconfirmed and the sound identity is the best matching reference sound.

If the best matching reference sound is a sound that is to be rejected ('Vacuum cleaner' or 'Child's Toy') then the Sound takes no further action. Otherwise the Sound sends a signal to the part of the ACU adapted to transmit information to the AMS via low power radio stating the sound identity and whether the sound identification is confirmed or unconfirmed.

The ACU then forwards this message to the monitoring station by means of wireline or wireless telephony.

This alert sending arrangement is shown in FIG. **4***a*.

The invention claimed is:

1. A monitoring and control system comprising:

a control unit for receiving signals from a variety of detection devices monitoring events pertaining to security, the control unit having means for transferring information related to the reception of such signals to a remote monitoring station and having control means for actively controlling one or more detection devices;

the monitoring station having programmable storage means storing automatic evaluation routines to initiate the automatic transfer of information to a chosen remote user terminal;

wherein the monitoring station is responsive to commands initiated by a remote user terminal, which is remote of the monitoring station and the site being monitored and which may be the chosen remote user terminal or an alternative remote user terminal, to establish a link between the remote user terminal and the control unit to cause the control means thereof to initiate a change in the operative state of at least one of the detection devices.

2. A system according to claim **1**, wherein the monitoring station is responsive to commands initiated by the remote user terminal, which may be the chosen remote user terminal or the alternative remote user terminal, to effect changes to the automatic evaluation routines.

3. A system according to claim **1**, wherein the monitoring station is responsive to a command request initiated by the remote user terminal to transfer additional information to the monitoring station and/or the remote user terminal.

4. A system according to claim **1** wherein the detection devices include fire or heat or CO sensors.

5. A system according to claim **1**, wherein the at least some detection devices generate audio signals or light signals differentiable in terms of frequency, intensity and/or time.

6. A system according to claim **1**, wherein the detection devices include or are supplemented by at least one video camera and video images are transferable to the monitoring station.

7. A system according to claim **1**, wherein the detection devices include at least one microphone and audible signals are transferable to the monitoring station.

8. A system according to claim **3**, wherein video images and/or audio signals represent the additional information.

9. A system according to claim 1, further comprising means for checking and evaluating the responses to events in relation to predetermined criteria to inhibit the transfer of information or modify automatic evaluation routines where detected events are deemed not significant.

10. A system according to claim 1, wherein the monitoring station is programmed to perform predetermined external control functions on the control unit.

11. A system according to claim 1, wherein the control unit is adapted to respond to the receipt of an initial signal indicating an event by transferring information immediately to the monitoring station and the monitoring station is adapted to wait for a short period of time after receipt to enable a cancellation command to be received to terminate the subsequent operation of the monitoring station.

12. A system according to claim 1, wherein the monitoring station independently serves to transfer messages and data to the control unit.

13. A control unit for use in the monitoring and control system of claim 1, said control unit comprising: interface means for receiving signals generated by detection devices in response to detectable events and means for transmitting information relating to received signals to the remote monitoring station.

14. A control unit according to claim 13 capable of receiving signals of the same general character from the variety of detection devices, wherein the control unit is equipped with or linked to means for differentiating or discriminating between such signals and the events which caused the signals.

15. A control unit according to claim 14, wherein the means for differentiating or discriminating between such signals and the events which caused the signals comprises a store of reference signals and means for receiving signals and comparing received signals to stored reference signals.

16. A control unit according to claim 15, wherein the store of reference signals includes alarm signals and non-alarm signals of the same general character.

17. A control unit according to claim 14 wherein the means for differentiating or discriminating between such signals and the events which caused the signals differentiates or discriminates between audible signals.

18. A control unit according to claim 14 wherein the means for differentiating or discriminating between such signals and the events which caused the signals differentiates or discriminates between visible signals.

19. A control unit according to claim 13, wherein the means for receiving signals and the means for transmitting information relating to received signals are located in different parts of a monitored site and are operably linked by wireless or wireline transmission.

20. An automatic monitoring station for receiving first information related to events detectable by detection devices, for use in a monitoring and control system according to claim 1, the monitoring station comprising means adapted to receive such first information and programmable storage means storing:

i) routines for evaluating received first information,

ii) a record of actions to be taken in response to a variety of types of evaluated first information,

iii) routines for matching evaluated first information to a particular stored action or set of actions, and

iv) routines for initiating the matched action or set of actions; wherein some actions include transferring second information relating to detected events to the chosen remote user terminal.

21. A monitoring and control system according to claim 1 further comprising an alarm control unit, said alarm control unit comprising:

i) a detector for receiving signals from the one or more pre-existing alarm systems;

ii) a communications module;

iii) means for recording reference samples of different signals produced by the one or more pre-existing alarm systems;

iv) means for distinguishing the signals from one another and from background interference, by comparing the detected signals or interference with the recorded reference signals; and

v) means for transmitting an output via the communications module.

22. A method of monitoring a site equipped with one or more detection devices for monitoring events pertaining to security and generating signals in response to detectable events, the method comprising:

utilizing a local control unit for receiving signals related to events pertaining to security, the local control unit having means for transferring information related to the reception of such signals to a remote monitoring station and having control means for actively controlling the one or more detection devices;

utilizing a monitoring station, remote from the local control unit, to initiate the automatic transfer of information to a chosen remote terminal in accordance with automatic evaluation routines programmed onto the monitoring station; and

enabling the monitoring station to respond to commands initiated from a remote user terminal, which is remote of the monitoring station and the site being monitored and which may be the chosen remote user terminal or an alternative remote user terminal, to establish a link between the remote user terminal and the control unit to cause the control means thereof to initiate a change in the operative state of at least one of the detection devices.

23. A method according to claim 22 further comprising enabling the monitoring station to respond to commands initiated from the remote user terminal, which may be the chosen remote user terminal or the alternative remote user terminal, to effect changes to the automatic evaluation routines.

24. A method according to claim 22 further comprising enabling the monitoring station to respond to a command request to transfer additional information to the monitoring station and/or the remote user terminal.

25. A method according to claim 22, wherein the local control unit or the monitoring station are adapted to determine the nature of the detected event prior to information being transferred to the remote terminal.

26. An alarm control unit (ACU) for use in combination with one or more pre-existing alarm systems, wherein the ACU comprises:

i) a detector for receiving signals from the one or more pre-existing alarm systems;

ii) a communications module;

iii) means for recording reference samples of different signals produced by the one or more pre-existing alarm systems;

iv) means for distinguishing the signals from one another and from background interference, by comparing the detected signals or interference with the recorded reference signals; and

v) means for transmitting an output via the communications module.

27. An ACU according to claim **26** wherein the signals are audible sound.

28. An ACU according to claim **27** wherein the detector is a microphone.

29. An ACU according to claim **26**, wherein the means for distinguishing the signals from one another and background interference is a speech-recognition chip.

30. An ACU according to claim **28** wherein the detector is a microphone and the microphone is intermittently activated and then deactivated, so that it detects sound in bursts with periods of silence before and after each burst; whereby the sound is adapted for interpretation by the speech recognition chip.

31. An ACU according to claim **30** wherein the period of activation is 1.5 seconds and the period of deactivation is 0.5 seconds.

32. An ACU according to claim **30**, wherein the speech recognition chip is an RSC 300 speech recognition chip.

33. An ACU according to claim **26** wherein, once the ACU has matched a signal to a reference sample, it transmits information relating to the signal to a monitoring station.

34. An ACU according to claim **33** wherein, the transmitted information indicates the particular signal that was detected.

35. An ACU according to claim **26**, wherein reference samples of background interference are recorded and compared with the detected signals or background interference.

* * * * *

EXHIBIT 3

US008335842B2

(12) **United States Patent**
Raji et al.

(10) **Patent No.: US 8,335,842 B2**
(45) **Date of Patent: Dec. 18, 2012**

(54) **PREMISES MANAGEMENT NETWORKING**

(75) Inventors: **Reza Raji**, Menlo Park, CA (US); **Gerald Gutt**, Tucson, AZ (US)

(73) Assignee: **iControl Networks, Inc.**, Redwood City, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 926 days.

(21) Appl. No.: **11/084,232**

(22) Filed: **Mar. 16, 2005**

(65) **Prior Publication Data**

US 2005/0216580 A1 Sep. 29, 2005

Related U.S. Application Data

(60) Provisional application No. 60/553,934, filed on Mar. 16, 2004, provisional application No. 60/553,932, filed on Mar. 16, 2004, provisional application No. 60/652,475, filed on Feb. 11, 2005.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/223**; 709/224; 709/225; 709/217; 709/218; 726/11; 726/12; 715/736; 700/17; 700/19

(58) **Field of Classification Search** 709/220, 709/223–225, 217–218; 715/736; 370/351; 379/102.01; 726/11–12; 340/3.1, 3.7, 3.71; 700/17, 19
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,754,261	A	6/1988	Marino	
4,779,007	A	10/1988	Schlanger et al.	
4,833,449	A	5/1989	Gaffigan	
4,860,185	A	8/1989	Brewer et al.	
4,993,059	A	2/1991	Smith et al.	
5,086,385	A	2/1992	Launey et al.	
5,519,878	A	5/1996	Dolin, Jr.	
5,579,197	A	11/1996	Mengelt et al.	
5,715,394	A *	2/1998	Jabs	709/223
5,907,279	A	5/1999	Bruins et al.	
5,963,916	A	10/1999	Kaplan	
D416,910	S	11/1999	Vasquez	
5,991,795	A	11/1999	Howard et al.	
6,037,991	A	3/2000	Thro et al.	
6,052,052	A	4/2000	Delmonaco	
6,060,994	A	5/2000	Chen	
6,134,591	A	10/2000	Nickles	

(Continued)

FOREIGN PATENT DOCUMENTS

JP	2003/085258 A	9/2001
JP	2003-85258 A	9/2001
JP	2003-141659	10/2001
JP	2003/141659	10/2001

(Continued)

OTHER PUBLICATIONS

Examination Report under Section 18(3), dated Aug. 13, 2007 re UK patent application No. GB0620362.4.

(Continued)

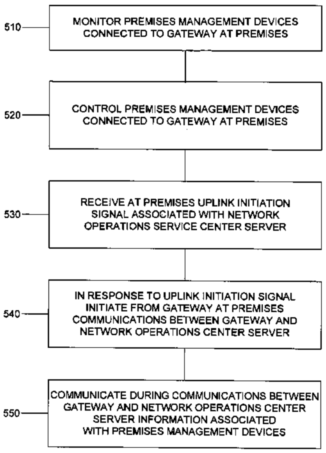
Primary Examiner — Alina N. Boutah

(74) *Attorney, Agent, or Firm* — Gregory & Sawrie LLP

(57) **ABSTRACT**

Some embodiments of a method for premises management networking include monitoring premises management devices connected to a gateway at a premises; controlling premises management devices connected to the gateway at the premises; receiving, at the premises, an uplink-initiation signal associated with a network operations center server; and in response to the uplink-initiation signal, initiating, from the gateway at the premises, communications between the gateway and the network operations center server; and communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices.

25 Claims, 17 Drawing Sheets


510
MONITOR PREMISES MANAGEMENT DEVICES CONNECTED TO GATEWAY AT PREMISES
520
CONTROL PREMISES MANAGEMENT DEVICES CONNECTED TO GATEWAY AT PREMISES
530
RECEIVE AT PREMISES UPLINK INITIATION SIGNAL ASSOCIATED WITH NETWORK OPERATIONS SERVICE CENTER SERVER
540
IN RESPONSE TO UPLINK INITIATION SIGNAL INITIATE FROM GATEWAY AT PREMISES COMMUNICATIONS BETWEEN GATEWAY AND NETWORK OPERATIONS CENTER SERVER
550
COMMUNICATE DURING COMMUNICATIONS BETWEEN GATEWAY AND NETWORK OPERATIONS CENTER SERVER INFORMATION ASSOCIATED WITH PREMISES MANAGEMENT DEVICES

U.S. PATENT DOCUMENTS

6,140,987	A	10/2000	Stein et al.	
6,198,479	B1	3/2001	Humpleman et al.	
6,219,677	B1	4/2001	Howard	
6,281,790	B1	8/2001	Kimmel et al.	
6,286,038	B1	9/2001	Reichmeyer et al.	
6,288,716	B1	9/2001	Humpleman et al.	
D451,529	S	12/2001	Vasquez	
6,331,122	B1	12/2001	Wu	
6,351,829	B1	2/2002	Dupont et al.	
6,353,891	B1	3/2002	Borella et al.	
6,363,417	B1	3/2002	Howard et al.	
6,363,422	B1 *	3/2002	Hunter et al.	709/224
6,370,436	B1	4/2002	Howard et al.	
6,377,861	B1	4/2002	York	
6,385,772	B1	5/2002	Courtney	
6,400,265	B1	6/2002	Saylor et al.	
D464,328	S	10/2002	Vasquez et al.	
D464,948	S	10/2002	Vasquez et al.	
6,462,507	B2	10/2002	Fisher, Jr.	
6,462,663	B1	10/2002	Wilson et al.	
6,467,084	B1	10/2002	Howard et al.	
6,480,901	B1	11/2002	Weber et al.	
6,493,020	B1	12/2002	Stevenson et al.	
6,496,927	B1	12/2002	McGrane	
6,529,723	B1	3/2003	Bentley	
6,542,075	B2	4/2003	Barker et al.	
6,563,800	B1	5/2003	Salo et al.	
6,574,234	B1	6/2003	Myer et al.	
6,580,950	B1	6/2003	Johnson et al.	
6,587,736	B2	7/2003	Howard et al.	
6,591,094	B1	7/2003	Bentley	
6,601,086	B1	7/2003	Howard et al.	
6,609,127	B1	8/2003	Lee et al.	
6,615,088	B1	9/2003	Myer et al.	
6,621,827	B1	9/2003	Rezvani et al.	
6,636,893	B1 *	10/2003	Fong	709/223
6,643,652	B2	11/2003	Helgeson et al.	
6,643,669	B1	11/2003	Novak et al.	
6,648,682	B1	11/2003	Wu	
6,658,091	B1	12/2003	Naidoo et al.	
6,661,340	B1	12/2003	Saylor et al.	
6,686,838	B1	2/2004	Rezvani et al.	
6,690,411	B2	2/2004	Naidoo et al.	
6,693,545	B2	2/2004	Brown et al.	
6,721,689	B2	4/2004	Markle et al.	
6,721,747	B2	4/2004	Lipkin	
6,738,824	B1	5/2004	Blair	
6,756,998	B1	6/2004	Bilger	
6,778,085	B2	8/2004	Faulkner et al.	
6,781,509	B1	8/2004	Oppedahl et al.	
6,789,147	B1	9/2004	Kessler et al.	
6,795,322	B2	9/2004	Aihara et al.	
6,798,344	B2	9/2004	Faulkner et al.	
6,826,233	B1	11/2004	Oosawa	
6,865,690	B2	3/2005	Kocin	
6,891,838	B1	5/2005	Petite et al.	
6,912,429	B1	6/2005	Bilger	
6,928,148	B2	8/2005	Simon et al.	
6,930,599	B2	8/2005	Naidoo et al.	
6,930,730	B2	8/2005	Maxon et al.	
6,931,445	B2	8/2005	Davis	
6,943,681	B2	9/2005	Rezvani et al.	
6,959,393	B2	10/2005	Hollis et al.	
6,965,313	B1	11/2005	Saylor et al.	
6,970,183	B1	11/2005	Monroe	
6,972,676	B1	12/2005	Kimmel et al.	
6,975,220	B1	12/2005	Foodman et al.	
6,990,591	B1	1/2006	Pearson	
7,016,970	B2	3/2006	Harumoto et al.	
7,020,697	B1 *	3/2006	Goodman et al.	709/223
7,020,701	B1 *	3/2006	Gelvin et al.	709/224
7,024,676	B1	4/2006	Klopfenstein	
7,030,752	B2	4/2006	Tyroler	
7,032,002	B1	4/2006	Rezvani et al.	
7,034,681	B2	4/2006	Yamamoto et al.	
7,039,391	B2	5/2006	Rezvani et al.	
7,047,088	B2	5/2006	Nakamura et al.	
7,047,092	B2	5/2006	Wimsatt	
7,072,934	B2	7/2006	Helgeson et al.	
7,079,020	B2	7/2006	Stilp	
7,080,046	B1	7/2006	Rezvani et al.	
7,085,937	B1	8/2006	Rezvani et al.	
7,099,944	B1	8/2006	Anschutz et al.	
7,103,152	B2	9/2006	Naidoo et al.	
7,106,176	B2	9/2006	La et al.	
7,113,090	B1	9/2006	Saylor et al.	
7,113,099	B2	9/2006	Tyroler et al.	
7,120,232	B2	10/2006	Naidoo et al.	
7,120,233	B2	10/2006	Naidoo et al.	
7,130,383	B2	10/2006	Naidoo et al.	
7,130,585	B1	10/2006	Ollis et al.	
7,148,810	B2 *	12/2006	Bhat	340/692
7,149,798	B2	12/2006	Rezvani et al.	
7,174,564	B1	2/2007	Weatherspoon et al.	
7,183,907	B2	2/2007	Simon et al.	
7,203,486	B2	4/2007	Patel	
7,209,945	B2 *	4/2007	Hicks et al.	709/203
7,218,217	B2	5/2007	Adonailo et al.	
7,222,359	B2	5/2007	Freund et al.	
7,237,267	B2	6/2007	Rayes et al.	
7,250,854	B2	7/2007	Rezvani et al.	
7,254,779	B1	8/2007	Rezvani et al.	
7,262,690	B2	8/2007	Heaton et al.	
7,305,461	B2	12/2007	Ullmann	
7,337,217	B2	2/2008	Wang	
7,337,473	B2	2/2008	Chang et al.	
7,343,619	B2	3/2008	Ofek et al.	
7,349,761	B1	3/2008	Cruse	
7,349,967	B2	3/2008	Wang	
7,367,045	B2	4/2008	Ofek et al.	
7,370,115	B2	5/2008	Bae et al.	
7,383,339	B1	6/2008	Meenan et al.	
7,403,838	B2	7/2008	Deen et al.	
7,409,451	B1	8/2008	Meenan et al.	
7,428,585	B1	9/2008	Owens et al.	
7,430,614	B2	9/2008	Shen et al.	
7,440,434	B2	10/2008	Chaskar et al.	
7,457,869	B2	11/2008	Kernan	
7,469,139	B2	12/2008	van de Groenendaal	
7,469,294	B1	12/2008	Luo et al.	
7,480,713	B2	1/2009	Ullmann	
7,480,724	B2	1/2009	Zimler et al.	
7,506,052	B2	3/2009	Qian et al.	
7,509,687	B2	3/2009	Ofek et al.	
7,526,762	B1	4/2009	Astala et al.	
7,551,071	B2	6/2009	Bennett, III et al.	
7,558,379	B2	7/2009	Winick	
7,577,420	B2	8/2009	Srinivasan et al.	
7,587,464	B2	9/2009	Moorer et al.	
7,627,665	B2	12/2009	Barker et al.	
7,634,519	B2	12/2009	Creamer et al.	
8,140,658	B1 *	3/2012	Gelvin et al.	709/224
2001/0016501	A1	8/2001	King	
2001/0034754	A1	10/2001	Elwahab et al.	
2002/0004828	A1	1/2002	Davis et al.	
2002/0026476	A1	2/2002	Miyazaki et al.	
2002/0029276	A1 *	3/2002	Bendinelli et al.	709/227
2002/0038380	A1	3/2002	Brawn et al.	
2002/0052913	A1	5/2002	Yamada et al.	
2002/0083342	A1	6/2002	Webb et al.	
2002/0095490	A1	7/2002	Barker et al.	
2002/0099809	A1 *	7/2002	Lee	709/223
2002/0103898	A1	8/2002	Moyer et al.	
2002/0103927	A1	8/2002	Parent	
2002/0107910	A1	8/2002	Zhao	
2002/0111698	A1	8/2002	Graziano et al.	
2002/0112051	A1	8/2002	Ullmann	
2002/0112182	A1	8/2002	Chang et al.	
2002/0128728	A1 *	9/2002	Murakami et al.	700/10
2002/0143923	A1 *	10/2002	Alexander	709/223
2002/0156564	A1	10/2002	Preston et al.	
2002/0180579	A1	12/2002	Nagaoka et al.	
2002/0184301	A1	12/2002	Parent	
2003/0005030	A1 *	1/2003	Sutton et al.	709/200
2003/0009552	A1	1/2003	Benfield et al.	
2003/0009553	A1	1/2003	Benfield et al.	
2003/0041137	A1 *	2/2003	Horie et al.	709/223

2003/0041167	A1	2/2003	French et al.	
2003/0051009	A1	3/2003	Shah et al.	
2003/0052923	A1	3/2003	Porter	
2003/0062997	A1 *	4/2003	Naidoo et al.	340/531
2003/0090473	A1	5/2003	Joshi	
2003/0115345	A1	6/2003	Chien et al.	
2003/0132018	A1	7/2003	Okita et al.	
2003/0174648	A1	9/2003	Wang	
2003/0187920	A1	10/2003	Redkar	
2003/0210126	A1	11/2003	Kanazawa	
2003/0236841	A1	12/2003	Epshteyn	
2004/0003241	A1	1/2004	Sengodan et al.	
2004/0015572	A1	1/2004	Kang	
2004/0037295	A1	2/2004	Tanaka et al.	
2004/0054789	A1	3/2004	Breh et al.	
2004/0086088	A1	5/2004	Naidoo et al.	
2004/0123149	A1	6/2004	Tyroler	
2004/0139227	A1	7/2004	Takeda	
2004/0162902	A1	8/2004	Davis	
2004/0177163	A1	9/2004	Casey et al.	
2004/0202351	A1 *	10/2004	Park et al.	382/104
2004/0243835	A1	12/2004	Terzis et al.	
2004/0267937	A1	12/2004	Klemets	
2005/0010866	A1 *	1/2005	Humpleman et al.	715/513
2005/0038326	A1	2/2005	Mathur	
2005/0066045	A1	3/2005	Johnson et al.	
2005/0069098	A1	3/2005	Kalervo et al.	
2005/0079855	A1	4/2005	Jethi et al.	
2005/0086126	A1	4/2005	Patterson	
2005/0102152	A1 *	5/2005	Hodges	705/1
2005/0108091	A1	5/2005	Sotak et al.	
2005/0108369	A1	5/2005	Sather et al.	
2005/0125083	A1	6/2005	Kiko	
2005/0128083	A1	6/2005	Puzio et al.	
2005/0149639	A1	7/2005	Vrielink et al.	
2005/0169288	A1	8/2005	Kamiwada et al.	
2005/0197847	A1 *	9/2005	Smith	705/1
2005/0216302	A1	9/2005	Raji et al.	
2005/0216580	A1 *	9/2005	Raji et al.	709/223
2005/0222820	A1	10/2005	Chung	
2005/0231349	A1	10/2005	Bhat	
2006/0009863	A1	1/2006	Lingemann	
2006/0064305	A1 *	3/2006	Alonso	705/1
2006/0088092	A1	4/2006	Chen et al.	
2006/0105713	A1	5/2006	Zheng et al.	
2006/0111095	A1	5/2006	Weigand	
2006/0181406	A1	8/2006	Petite et al.	
2006/0182100	A1	8/2006	Li et al.	
2006/0187900	A1	8/2006	Akbar	
2006/0200845	A1	9/2006	Foster et al.	
2006/0206220	A1	9/2006	Amundson	
2006/0271695	A1	11/2006	Lavian	
2006/0282886	A1	12/2006	Gaug	
2007/0052675	A1	3/2007	Chang	
2007/0061266	A1	3/2007	Moore et al.	
2007/0106124	A1	5/2007	Kuriyama et al.	
2007/0142022	A1	6/2007	Madonna et al.	
2007/0256105	A1	11/2007	Tabe	
2007/0286210	A1	12/2007	Gutt et al.	
2007/0286369	A1	12/2007	Gutt et al.	
2007/0298772	A1	12/2007	Owen et al.	
2008/0042826	A1	2/2008	Hevia et al.	
2008/0065681	A1	3/2008	Fontijn et al.	
2008/0084296	A1	4/2008	Kutzik et al.	
2008/0147834	A1	6/2008	Quinn et al.	
2008/0180240	A1	7/2008	Raji et al.	
2008/0183842	A1	7/2008	Raji et al.	
2008/0235326	A1	9/2008	Parsi et al.	
2009/0070436	A1	3/2009	Dawes et al.	
2009/0165114	A1	6/2009	Baum et al.	
2009/0204693	A1	8/2009	Andreev et al.	
2009/0240787	A1	9/2009	Denny	
2009/0240814	A1	9/2009	Brubacher et al.	
2010/0082744	A1	4/2010	Gutt et al.	
2010/0095111	A1	4/2010	Gutt	
2010/0095369	A1	4/2010	Gutt	

FOREIGN PATENT DOCUMENTS

JP	2004-192659	2/2004
JP	2004/192659	2/2004
KR	2006/0021605	9/2004
KR	2006-0021605	9/2004
WO	WO 89/07855	8/1989
WO	WO 01/52478	7/2001
WO	WO-01-52478	7/2001
WO	WO-01-99078	12/2001
WO	WO 01/99078	12/2001
WO	WO 2004/004222	1/2004
WO	WO-2004-004222	1/2004
WO	WO-2004-107710	12/2004
WO	WO 2004/107710	12/2004
WO	WO/2005/091218	9/2005
WO	WO 2005/091218 A2	9/2005
WO	WO 2005/091218 A3	9/2005

OTHER PUBLICATIONS

Examination Report under Section 18(3) re UK patent application No. GB0724760.4 dated Jan. 30, 2008.
Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jan. 30, 2008.
Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jun. 4, 2008.
Examination Report under Section 18(3) re UK patent application No. GB0800040.8 dated Jan. 30, 2008.
U.S. Appl. No. 12/630,092 Office Action mailed Jul. 21, 2010.
U.S. Appl. No. 12/019,568 Office Action mailed Jul. 13, 2010.
U.S. Appl. No. 12/019,554 Office Action mailed Jul. 12, 2010.
U.S. Appl. No. 12/019,554 Office Action mailed Jan. 5, 2010.
Form PCT/ISA/220, "PCT Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.
Form PCT/ISA/210, "PCT International Search Report," 2 pgs.
Form PCT/ISA/237, "PCT Written Opinion of the International Searching Authority," 8 pgs.
Form PCT/ISA/237, "PCT Written Opinion of the International Searching Authority," 6 pgs.
Form PCT/ISA/237, "PCT Written Opinion of the International Searching Authority," 7 pgs.
Form PCT/ISA/220, PCT/US05/08766, "PCT Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.
Form PCT/ISA/210, PCT/US05/08766, "PCT International Search Report," 2 pgs.
Form PCT/ISA/237, PCT/US05/08766, "PCT Written Opinion of the International Searching Authority," 5 pgs.
Examination Report under Section 18(3) re UK patent application No. GB0724760.4 dated Jan. 30, 2008 4 pgs.
Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jan. 30, 2008 4 pgs.
Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jun. 4, 2008 2 pgs.
Examination Report under Section 18(3) re UK patent application No. GB0800040.8 dated Jan. 30, 2008 4 pgs.
Examination Report under Section 18(3) re UK patent application No. GB0620362.4 dated Aug. 13, 2007, 3 pgs.
Alarm.com—Interactive Security Systems, Product Advantages, printed from website Nov. 4, 2003, 3 pp.
Alarm.com—Interactive Security Systems, Frequently Asked Questions, printed from website Nov. 4, 2003, 3 pp.
Alarm.com—Interactive Security Systems, Elders, printed from website Nov. 4, 2003, 1 page.
Alarm.com—Interactive Security Systems, Overview, printed from website Nov. 4, 2003, 2 pp.
X10—ActiveHome, Home Automation Made Easy!, printed from website Nov. 4, 2003, 3 pp.
Form PCT/ISA/220, "PCT Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.
Form PCT/SA/220, "PCT Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.

* cited by examiner

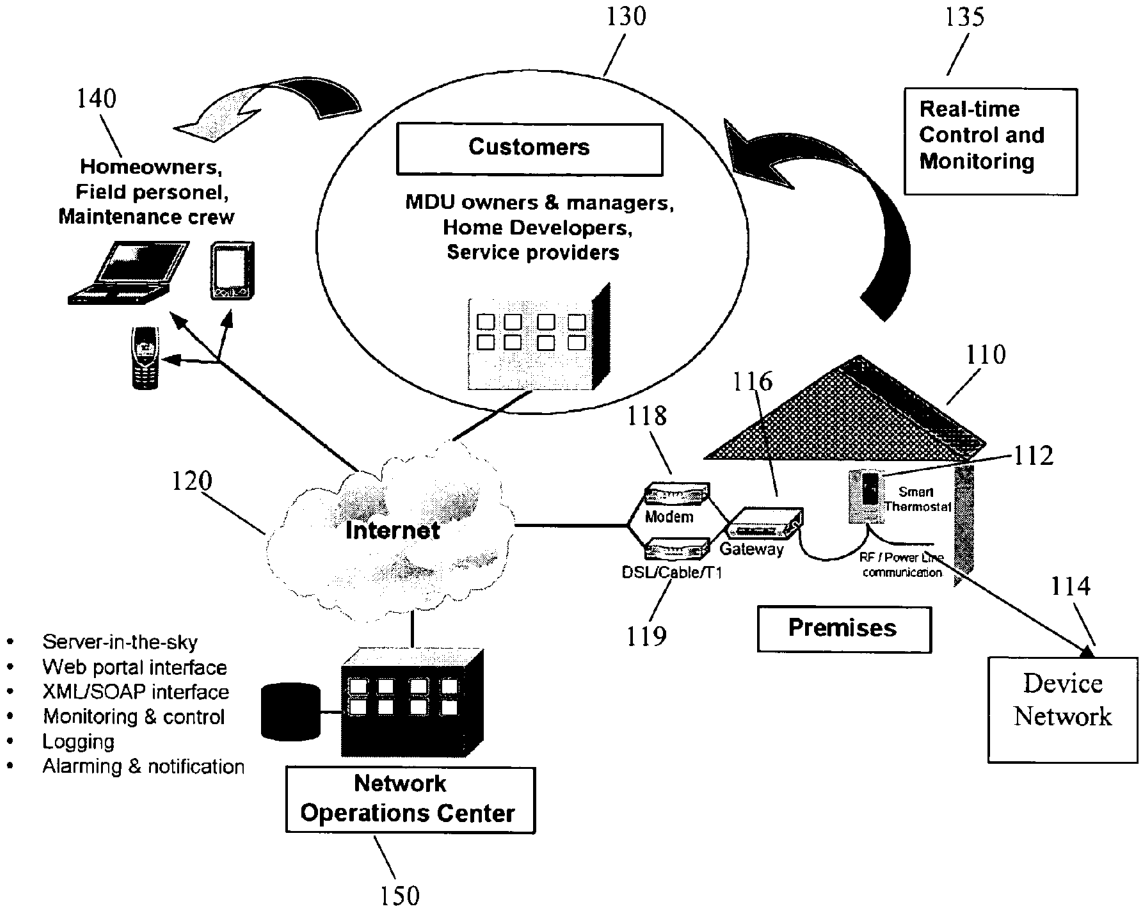

130
135
Real-time Control and Monitoring
140
Homeowners, Field personel, Maintenance crew
Customers
MDU owners & managers, Home Developers, Service providers
110
116
118
112
Smart Thermostat
120
Internet
Modem
Gateway
DSL/Cable/T1
RF / Power Line communication
114
119
Premises
Device Network
Server-in-the-sky
Web portal interface
XML/SOAP interface
Monitoring & control
Logging
Alarming & notification
Network Operations Center
150

FIGURE 1

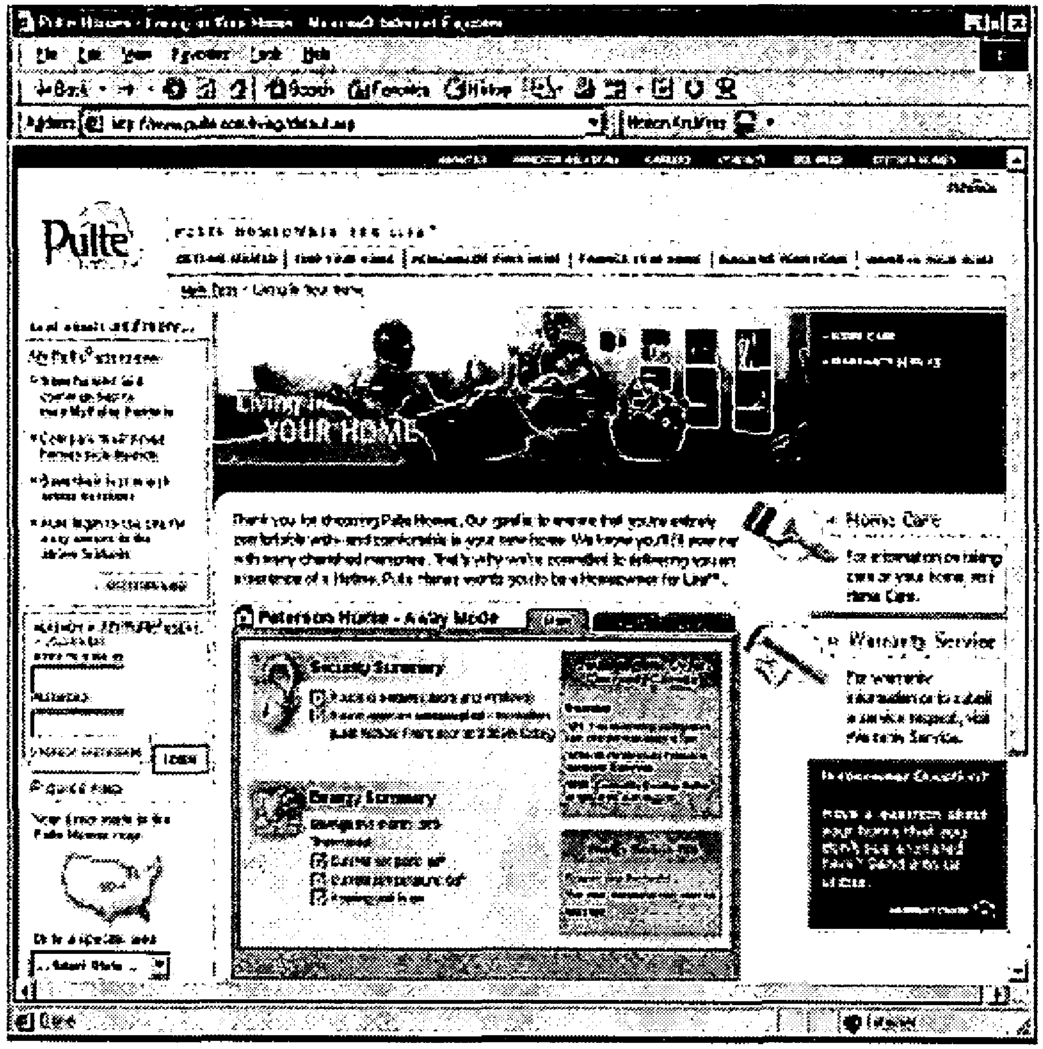

Living in YOUR HOME
Home Care
Warranty Service
Security Summary
Energy Summary

FIGURE 2

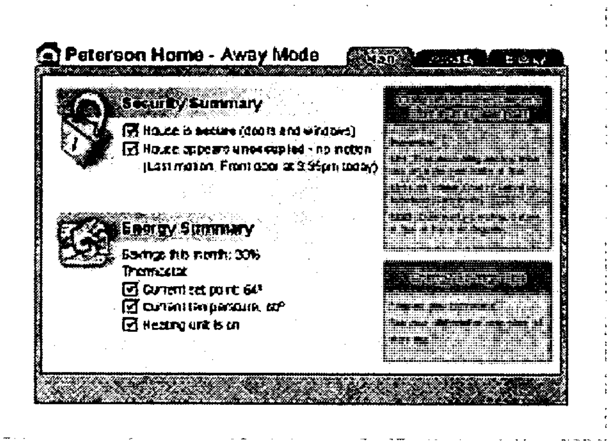

Peterson Home - Away Mode
Security Summary
House is secure (doors and windows)
Energy Summary
Thermostat
Heating unit is on

FIGURE 3A

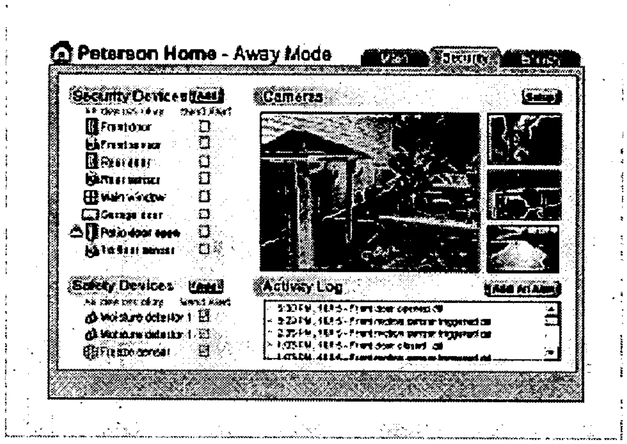

Peterson Home - Away Mode
Security Devices
Cameras
Front door
Safety Devices
Activity Log
Add An Alert

FIGURE 3B

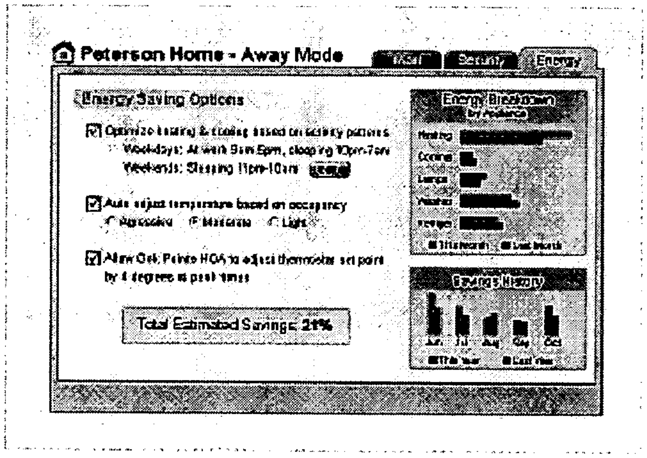

Peterson Home - Away Mode
Energy
Energy Saving Options
Energy Breakdown by Appliance
Savings History
Total Estimated Savings: 21%

FIGURE 3C

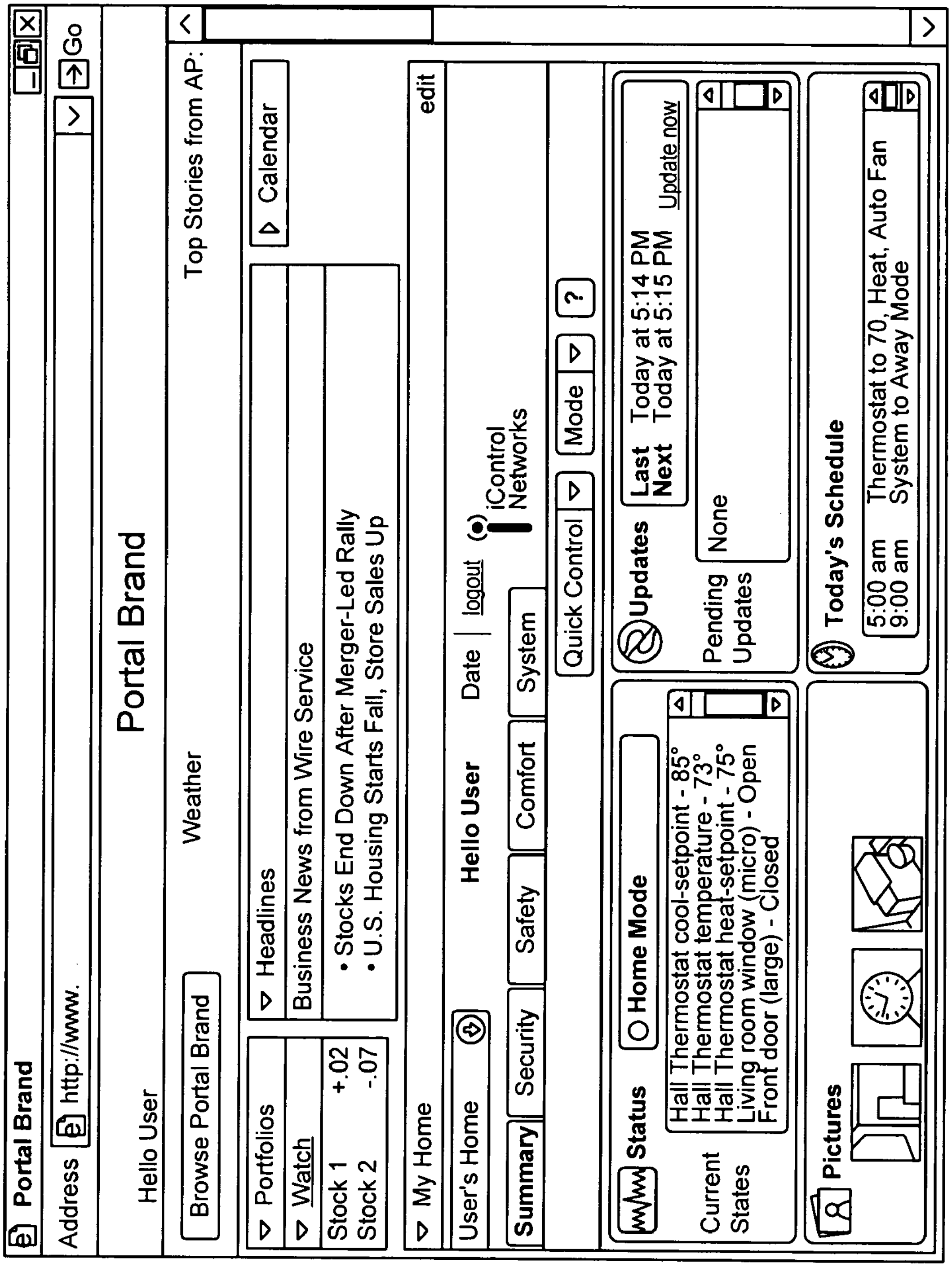

Portal Brand
Address http://www.
Go
Hello User
Portal Brand
Browse Portal Brand
Weather
Top Stories from AP:
Portfolios
Watch
Stock 1 +.02
Stock 2 -.07
Headlines
Business News from Wire Service
• Stocks End Down After Merger-Led Rally
• U.S. Housing Starts Fall, Store Sales Up
Calendar
My Home
edit
User's Home
Hello User
Date
logout
iControl Networks
Summary
Security
Safety
Comfort
System
Quick Control
Mode
?
Status
Home Mode
Current States
Hall Thermostat cool-setpoint - 85°
Hall Thermostat temperature - 73°
Hall Thermostat heat-setpoint - 75°
Living room window (micro) - Open
Front door (large) - Closed
Updates
Last Today at 5:14 PM
Next Today at 5:15 PM
Update now
Pending Updates
None
Pictures
Today's Schedule
5:00 am Thermostat to 70, Heat, Auto Fan
9:00 am System to Away Mode

Figure 3D

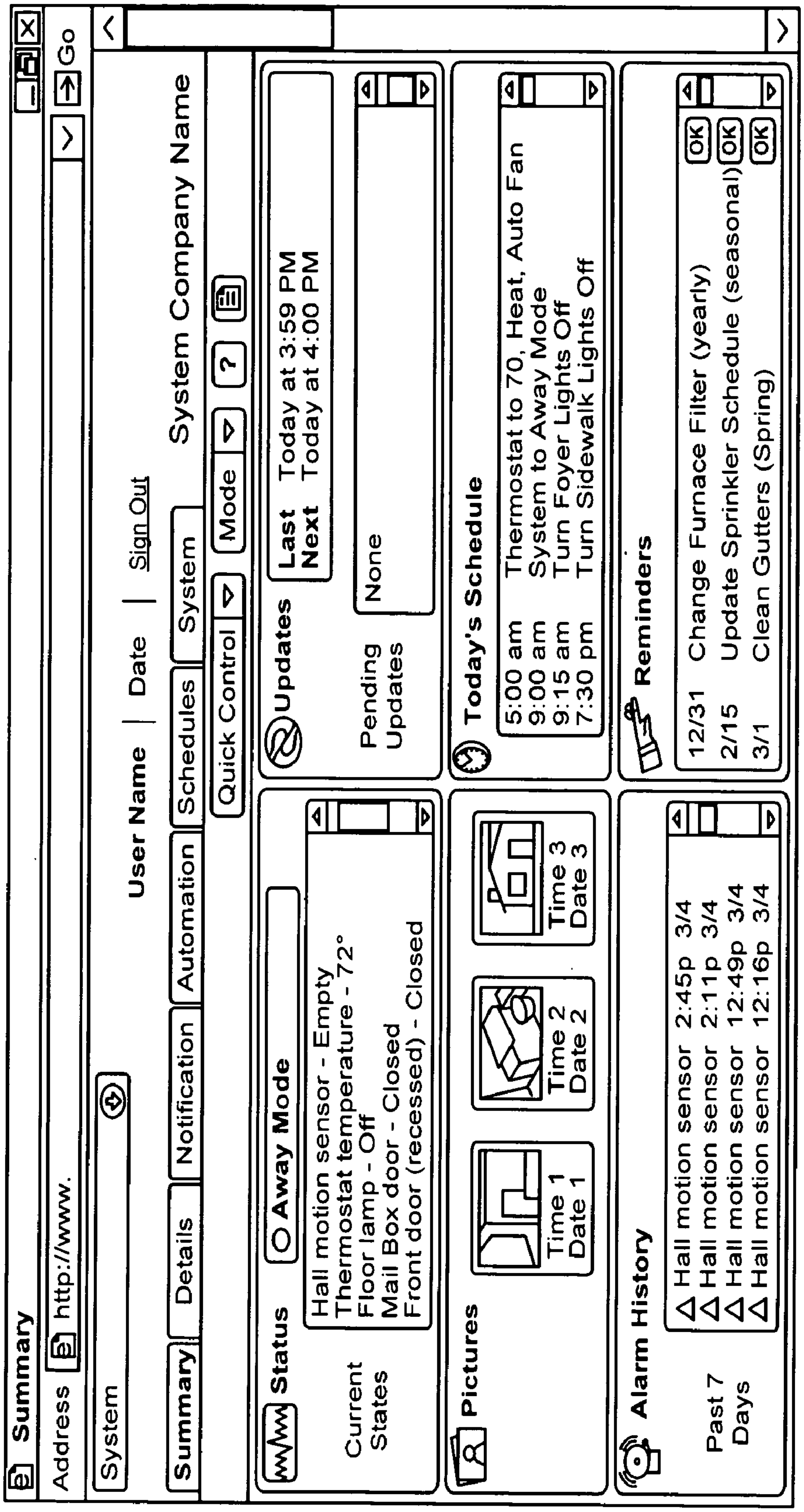

Summary
Address http://www.
Go
System
User Name | Date | Sign Out
System Company Name
Summary
Details
Notification
Automation
Schedules
System
Quick Control
Mode
Status
Away Mode
Current States
Hall motion sensor - Empty
Thermostat temperature - 72°
Floor lamp - Off
Mail Box door - Closed
Front door (recessed) - Closed
Updates
Last Today at 3:59 PM
Next Today at 4:00 PM
Pending Updates
None
Pictures
Time 1
Date 1
Time 2
Date 2
Time 3
Date 3
Today's Schedule
5:00 am Thermostat to 70, Heat, Auto Fan
9:00 am System to Away Mode
9:15 am Turn Foyer Lights Off
7:30 pm Turn Sidewalk Lights Off
Alarm History
Past 7 Days
Hall motion sensor 2:45p 3/4
Hall motion sensor 2:11p 3/4
Hall motion sensor 12:49p 3/4
Hall motion sensor 12:16p 3/4
Reminders
12/31 Change Furnace Filter (yearly) OK
2/15 Update Sprinkler Schedule (seasonal) OK
3/1 Clean Gutters (Spring) OK

Figure 3E

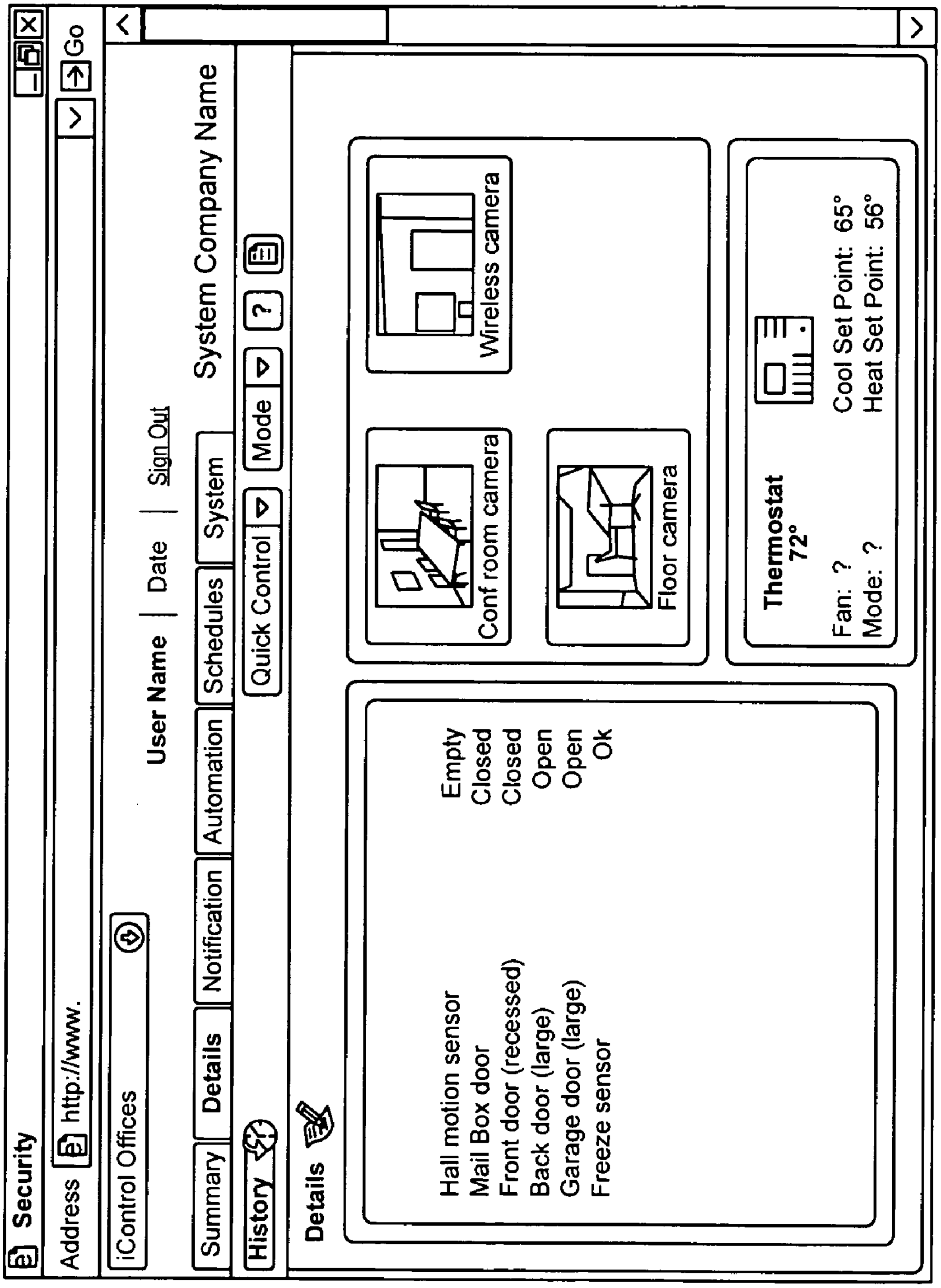

Security
Address
http://www.
Go
iControl Offices
User Name
Date
Sign Out
System Company Name
Summary
Details
Notification
Automation
Schedules
System
History
Quick Control
Mode
Details
Hall motion sensor Empty
Mail Box door Closed
Front door (recessed) Closed
Back door (large) Open
Garage door (large) Open
Freeze sensor Ok
Conf room camera
Wireless camera
Floor camera
Thermostat
72°
Fan: ?
Mode: ?
Cool Set Point: 65°
Heat Set Point: 56°

Figure 3F

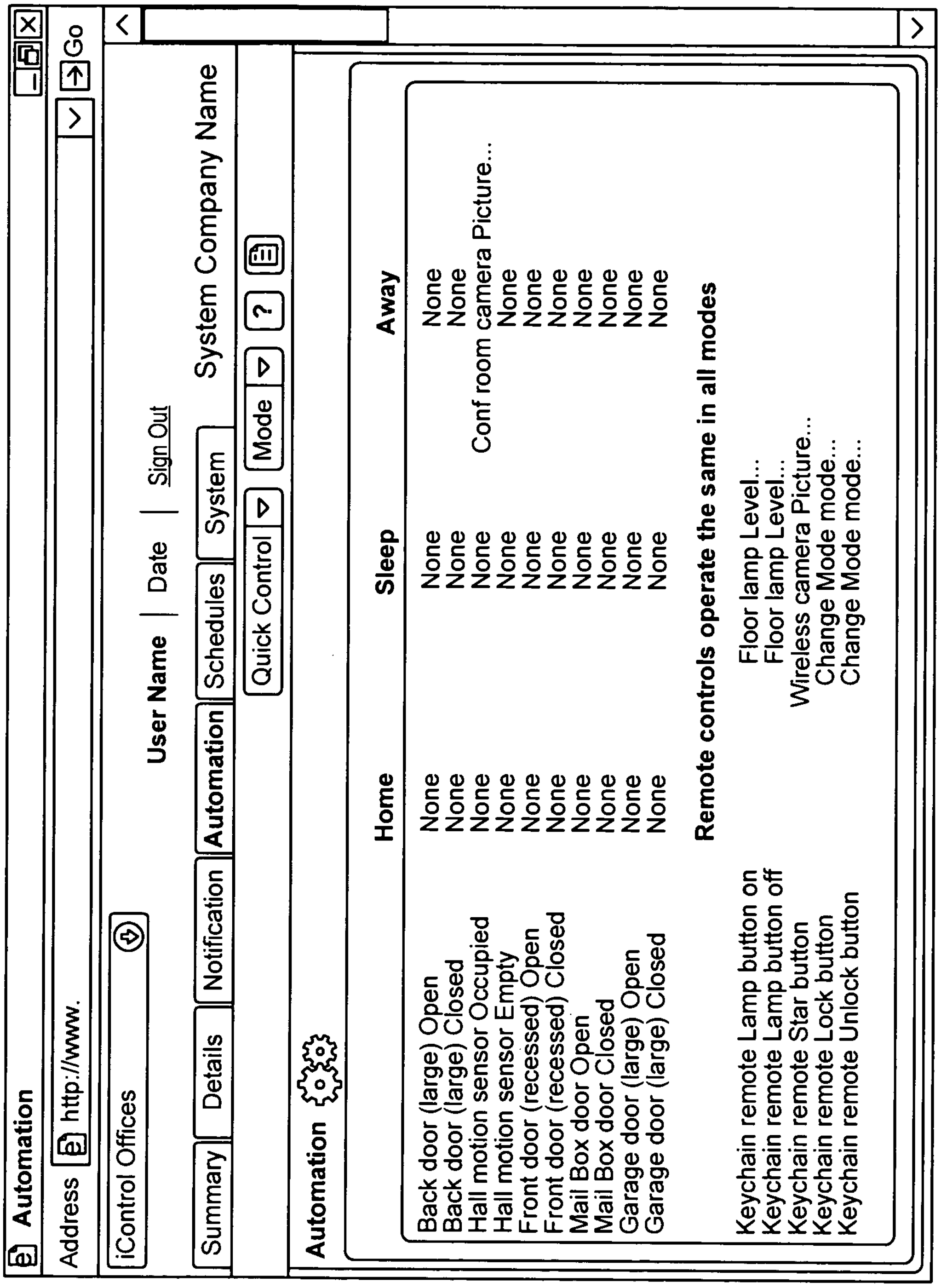

Automation
Address http://www.
Go
iControl Offices
User Name | Date | Sign Out
System Company Name
Summary
Details
Notification
Automation
Schedules
System
Quick Control
Mode
?
Automation
Home
Sleep
Away
Back door (large) Open None None None
Back door (large) Closed None None None
Hall motion sensor Occupied None None Conf room camera Picture...
Hall motion sensor Empty None None None
Front door (recessed) Open None None None
Front door (recessed) Closed None None None
Mail Box door Open None None None
Mail Box door Closed None None None
Garage door (large) Open None None None
Garage door (large) Closed None None None
Remote controls operate the same in all modes
Keychain remote Lamp button on Floor lamp Level...
Keychain remote Lamp button off Floor lamp Level...
Keychain remote Star button Wireless camera Picture...
Keychain remote Lock button Change Mode mode...
Keychain remote Unlock button Change Mode mode...

Figure 3G

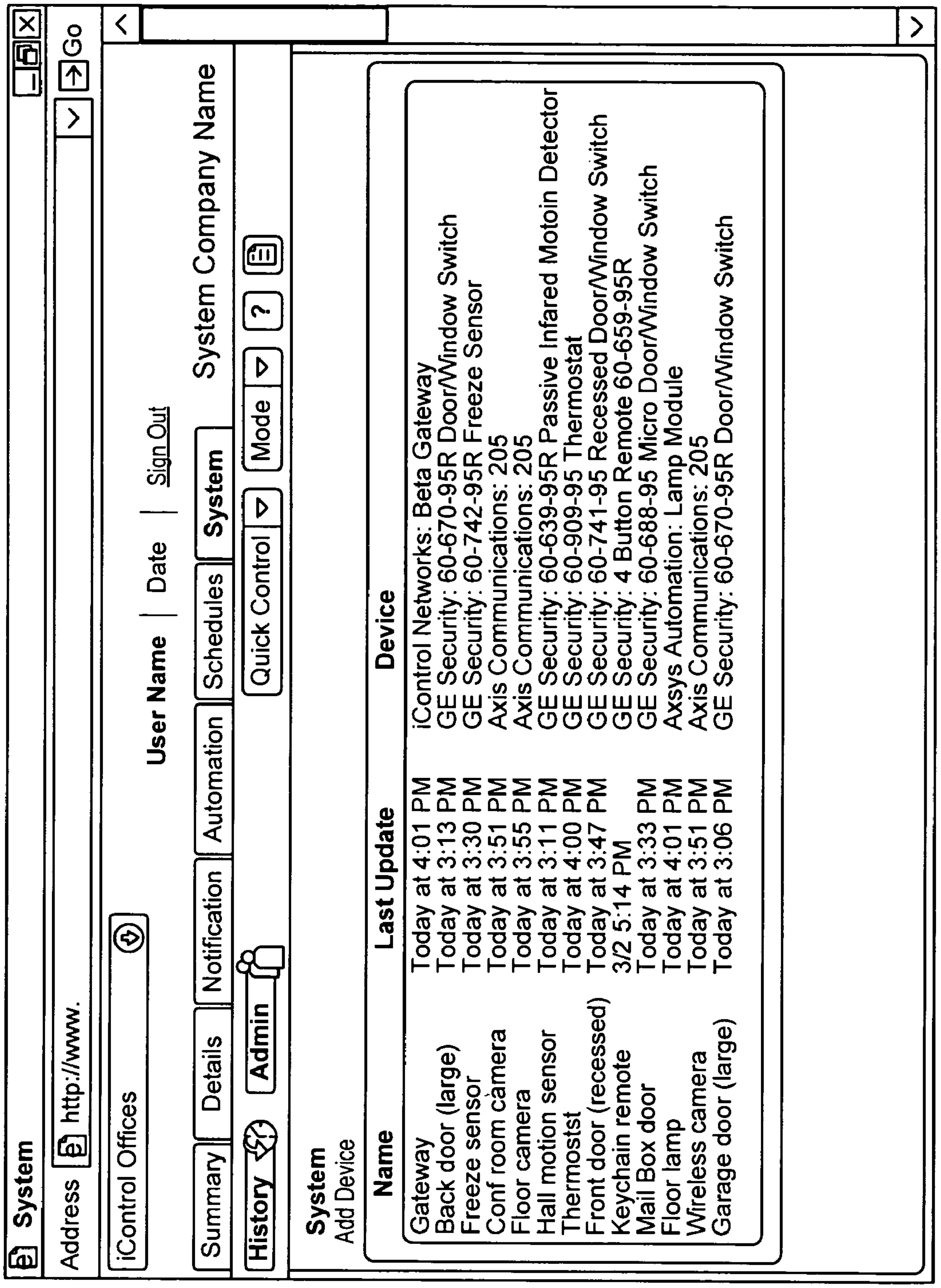

System
Address http://www.
Go
iControl Offices
User Name | Date | Sign Out
System Company Name
Summary
Details
Notification
Automation
Schedules
System
History
Admin
Quick Control
Mode
?
System
Add Device
Name
Last Update
Device
Gateway
Today at 4:01 PM
iControl Networks: Beta Gateway
Back door (large)
Today at 3:13 PM
GE Security: 60-670-95R Door/Window Switch
Freeze sensor
Today at 3:30 PM
GE Security: 60-742-95R Freeze Sensor
Conf room camera
Today at 3:51 PM
Axis Communications: 205
Floor camera
Today at 3:55 PM
Axis Communications: 205
Hall motion sensor
Today at 3:11 PM
GE Security: 60-639-95R Passive Infared Motoin Detector
Thermostst
Today at 4:00 PM
GE Security: 60-909-95 Thermostat
Front door (recessed)
Today at 3:47 PM
GE Security: 60-741-95 Recessed Door/Window Switch
Keychain remote
3/2 5:14 PM
GE Security: 4 Button Remote 60-659-95R
Mail Box door
Today at 3:33 PM
GE Security: 60-688-95 Micro Door/Window Switch
Floor lamp
Today at 4:01 PM
Axsys Automation: Lamp Module
Wireless camera
Today at 3:51 PM
Axis Communications: 205
Garage door (large)
Today at 3:06 PM
GE Security: 60-670-95R Door/Window Switch

Figure 3H

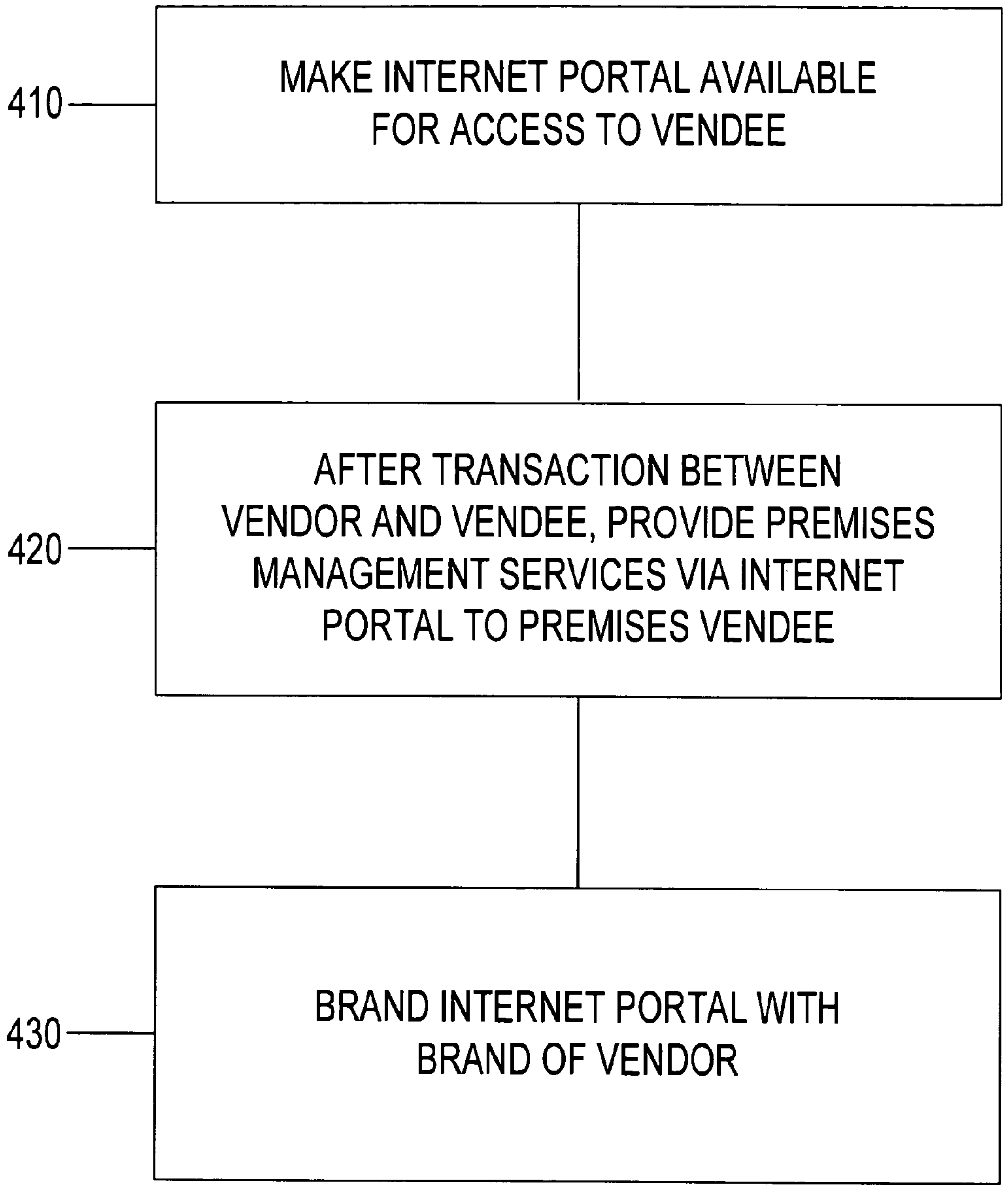

410
MAKE INTERNET PORTAL AVAILABLE FOR ACCESS TO VENDEE
420
AFTER TRANSACTION BETWEEN VENDOR AND VENDEE, PROVIDE PREMISES MANAGEMENT SERVICES VIA INTERNET PORTAL TO PREMISES VENDEE
430
BRAND INTERNET PORTAL WITH BRAND OF VENDOR

FIGURE 4

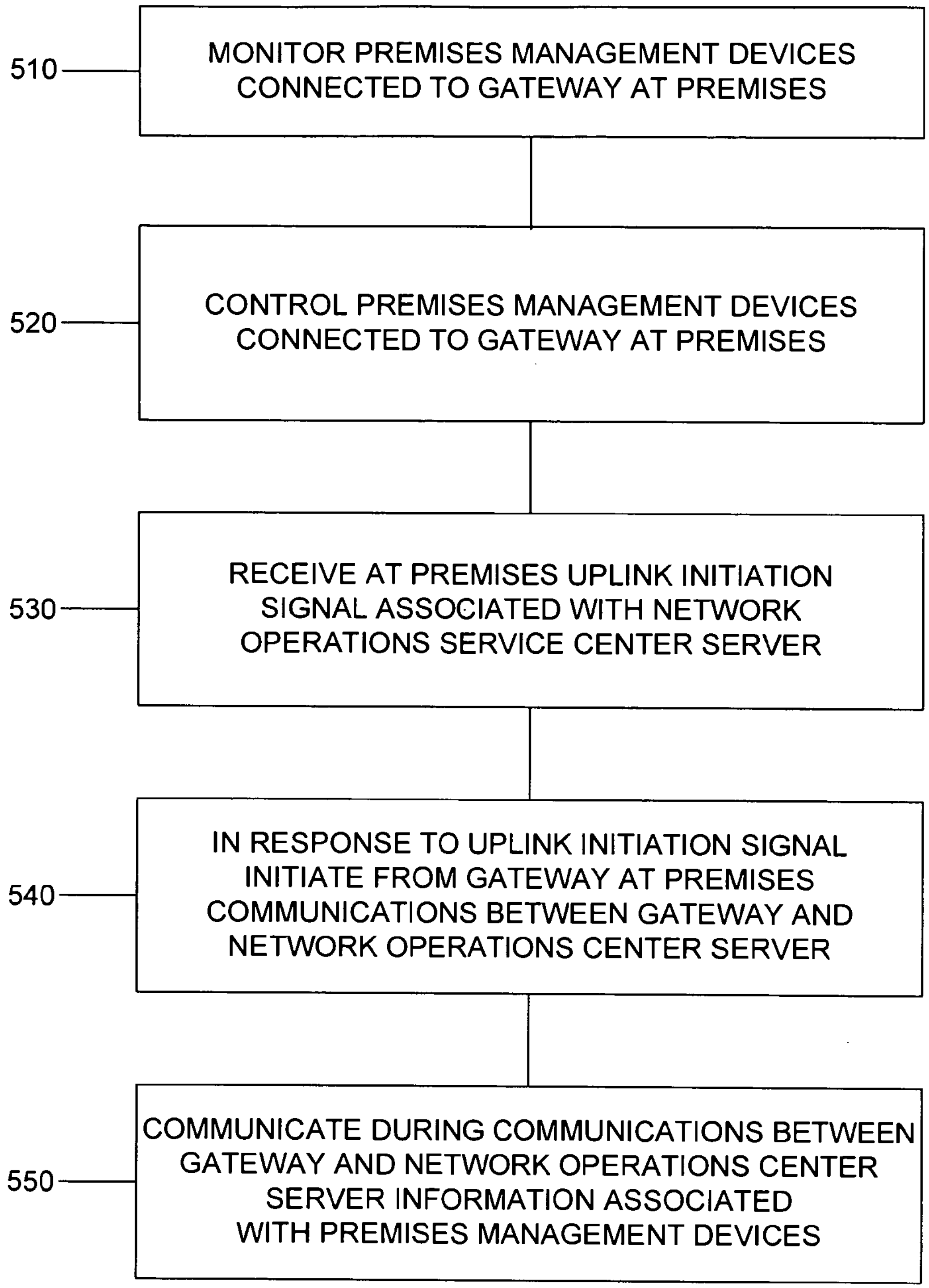

510
MONITOR PREMISES MANAGEMENT DEVICES CONNECTED TO GATEWAY AT PREMISES
520
CONTROL PREMISES MANAGEMENT DEVICES CONNECTED TO GATEWAY AT PREMISES
530
RECEIVE AT PREMISES UPLINK INITIATION SIGNAL ASSOCIATED WITH NETWORK OPERATIONS SERVICE CENTER SERVER
540
IN RESPONSE TO UPLINK INITIATION SIGNAL INITIATE FROM GATEWAY AT PREMISES COMMUNICATIONS BETWEEN GATEWAY AND NETWORK OPERATIONS CENTER SERVER
550
COMMUNICATE DURING COMMUNICATIONS BETWEEN GATEWAY AND NETWORK OPERATIONS CENTER SERVER INFORMATION ASSOCIATED WITH PREMISES MANAGEMENT DEVICES

FIGURE 5

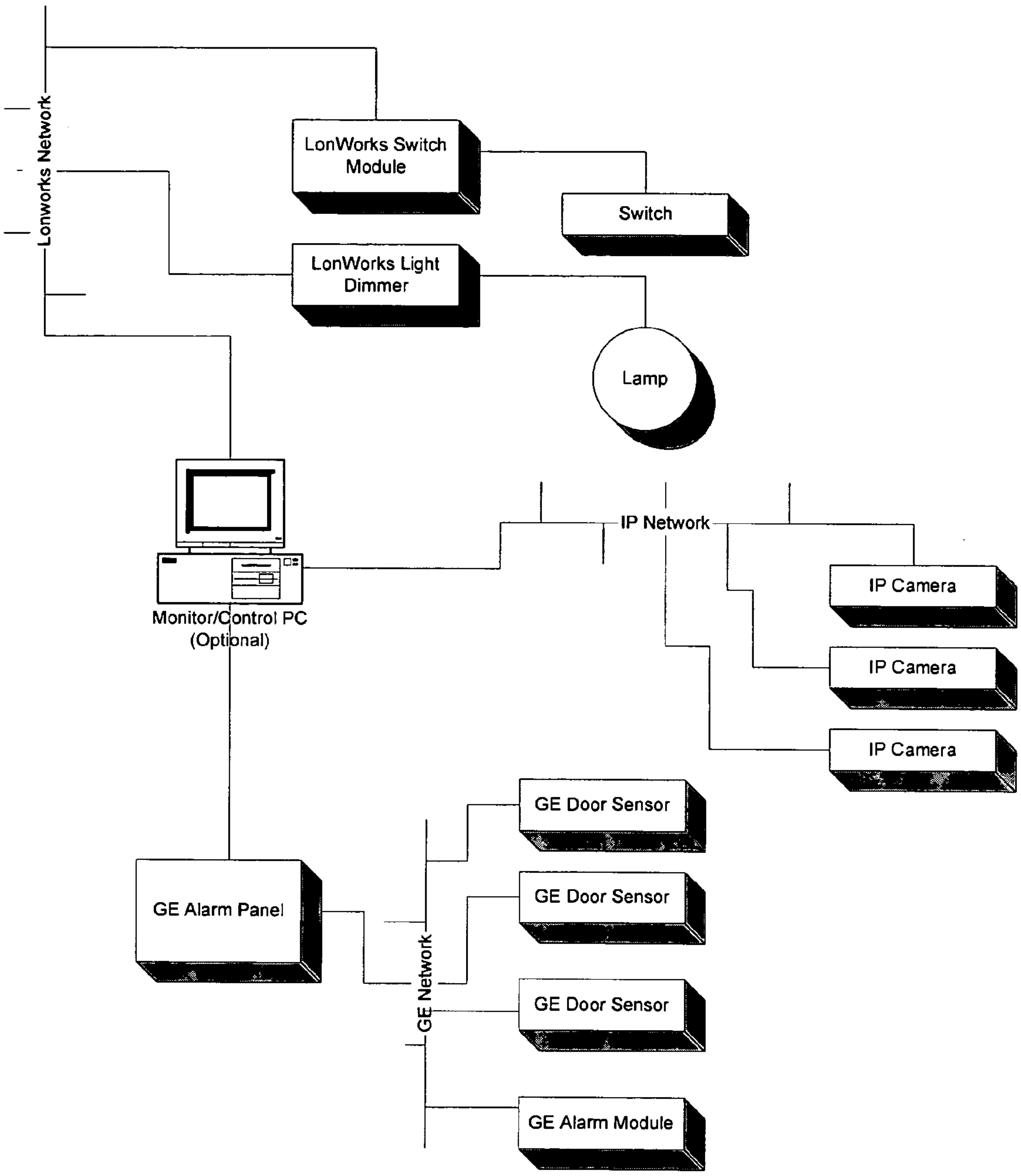

Lonworks Network
LonWorks Switch Module
Switch
LonWorks Light Dimmer
Lamp
Monitor/Control PC (Optional)
IP Network
IP Camera
IP Camera
IP Camera
GE Door Sensor
GE Door Sensor
GE Door Sensor
GE Alarm Module
GE Alarm Panel
GE Network

Figure 6

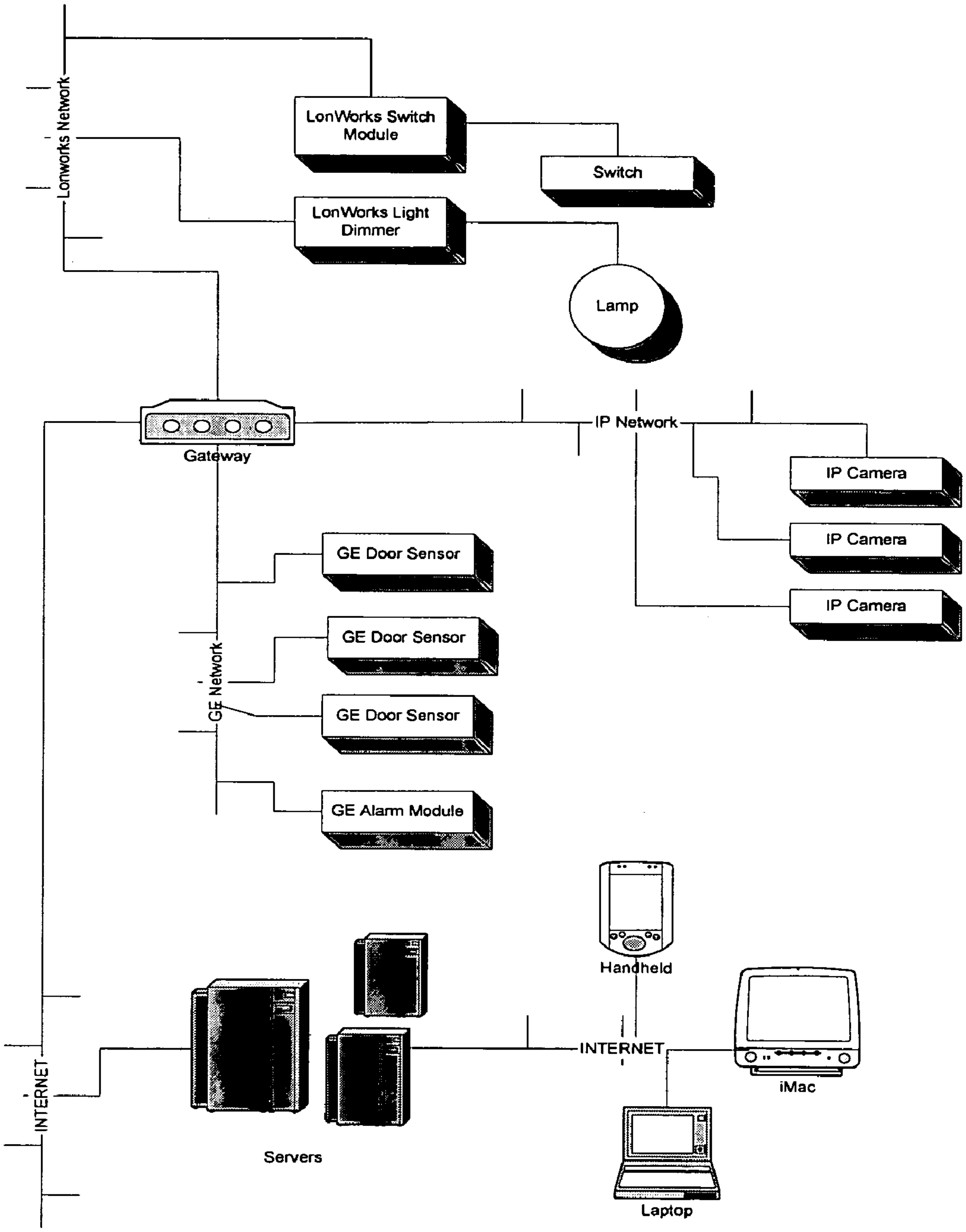
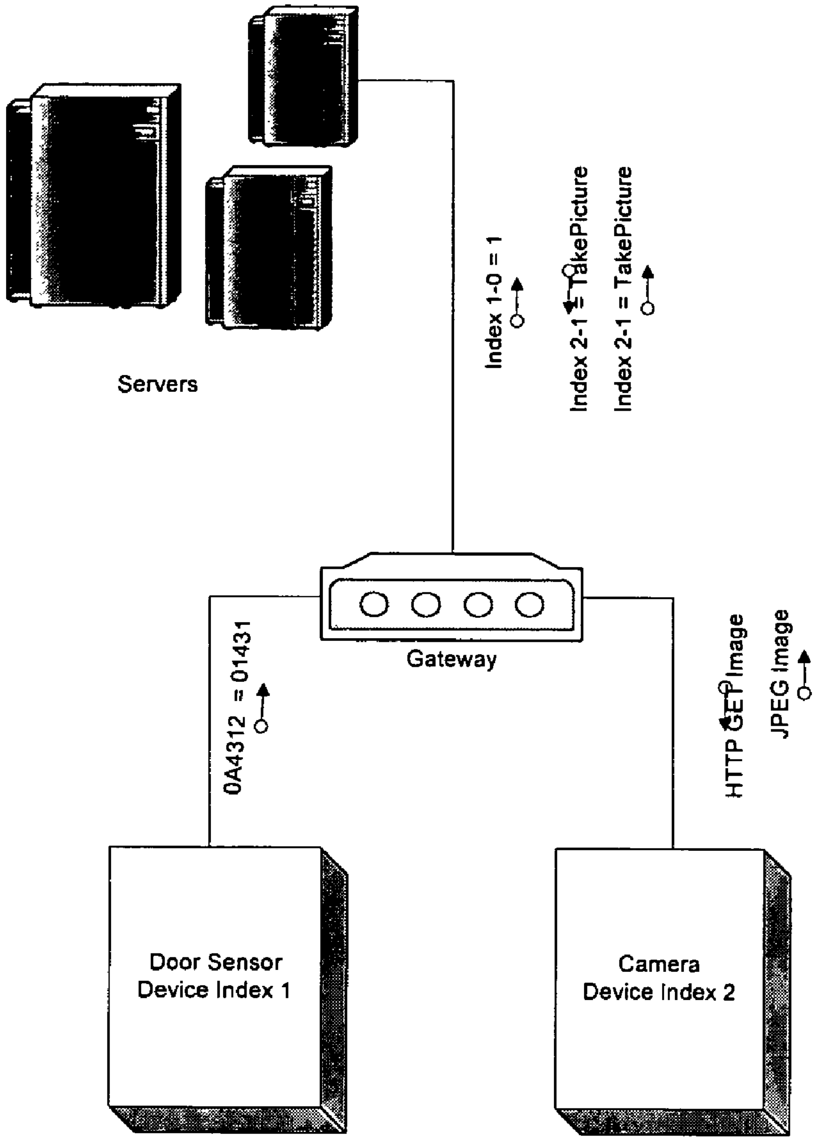

Lonworks Network
LonWorks Switch Module
Switch
LonWorks Light Dimmer
Lamp
Gateway
IP Network
IP Camera
IP Camera
IP Camera
GE Door Sensor
GE Door Sensor
GE Door Sensor
GE Alarm Module
GE Network
Handheld
INTERNET
iMac
Laptop
Servers
INTERNET

Figure 7 - System Architecture



Servers
Index 1-0 = 1
Index 2-1 = TakePicture
Index 2-1 = TakePicture
Gateway
0A4312 = 01431
HTTP GET Image
JPEG Image
Door Sensor
Device Index 1
Camera
Device Index 2

Figure 8 - Gateway Data Handling

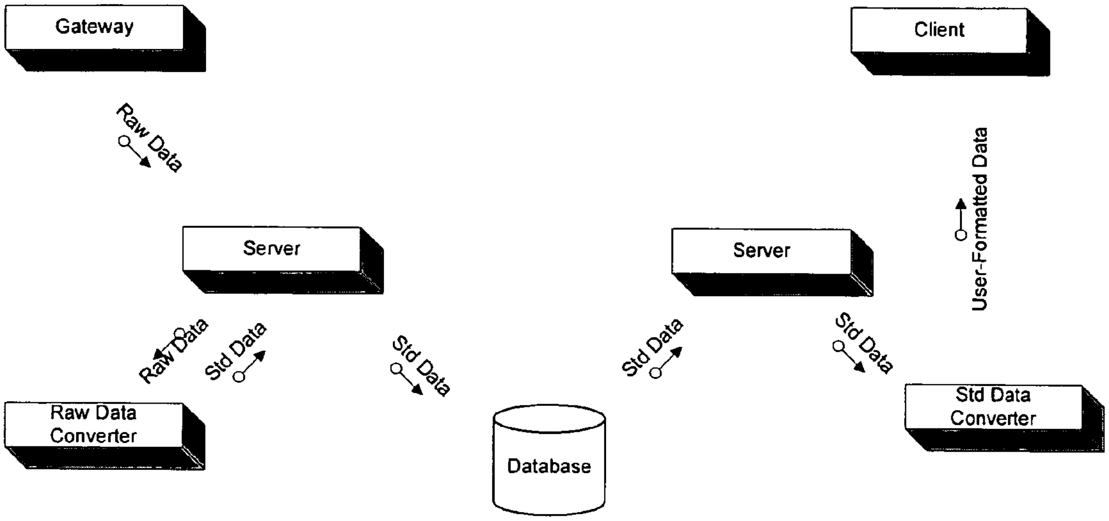

Gateway
Raw Data
Server
Raw Data
Std Data
Raw Data
Converter
Std Data
Database
Client
User-Formatted Data
Server
Std Data
Std Data
Std Data
Converter

Figure 9 - Data Conversion

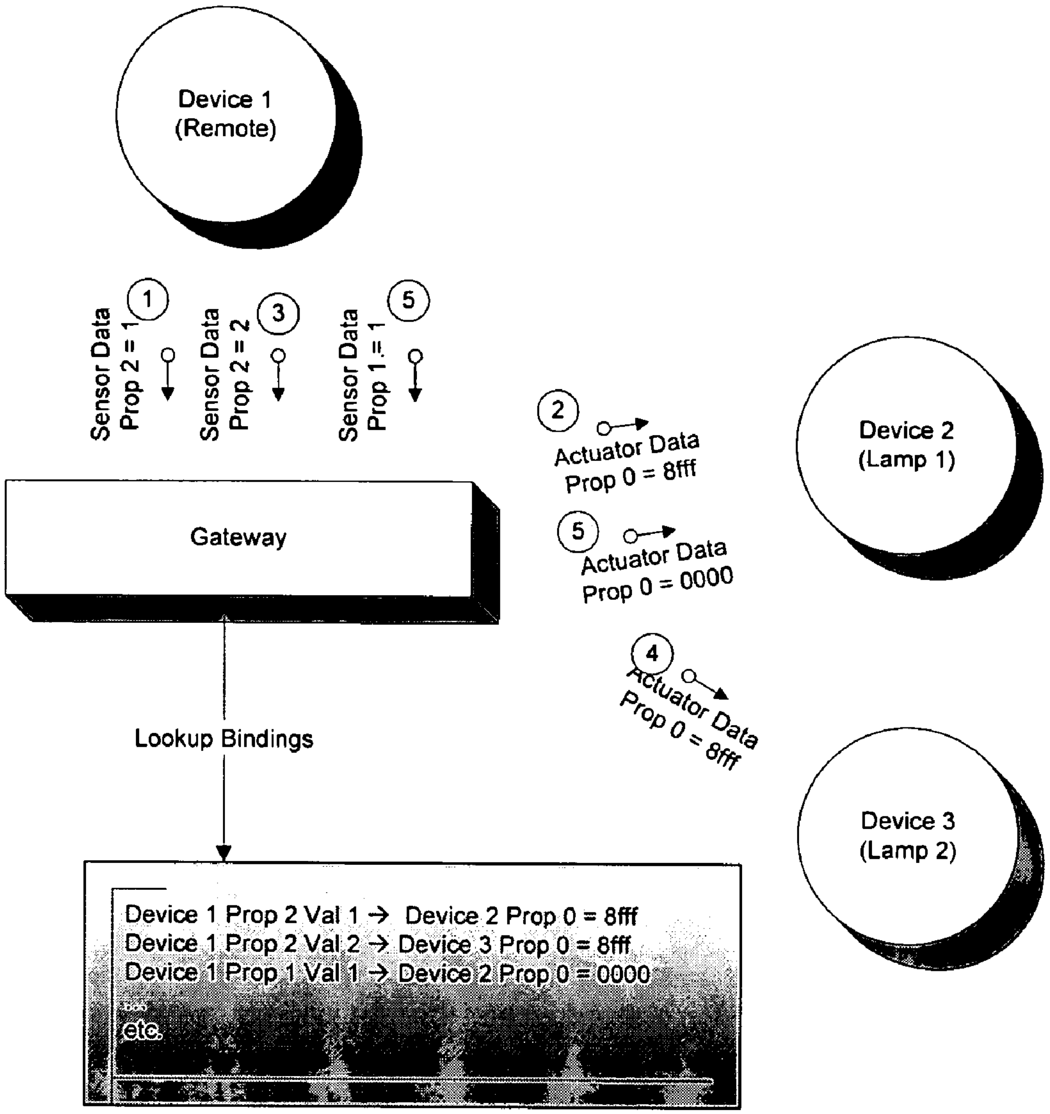
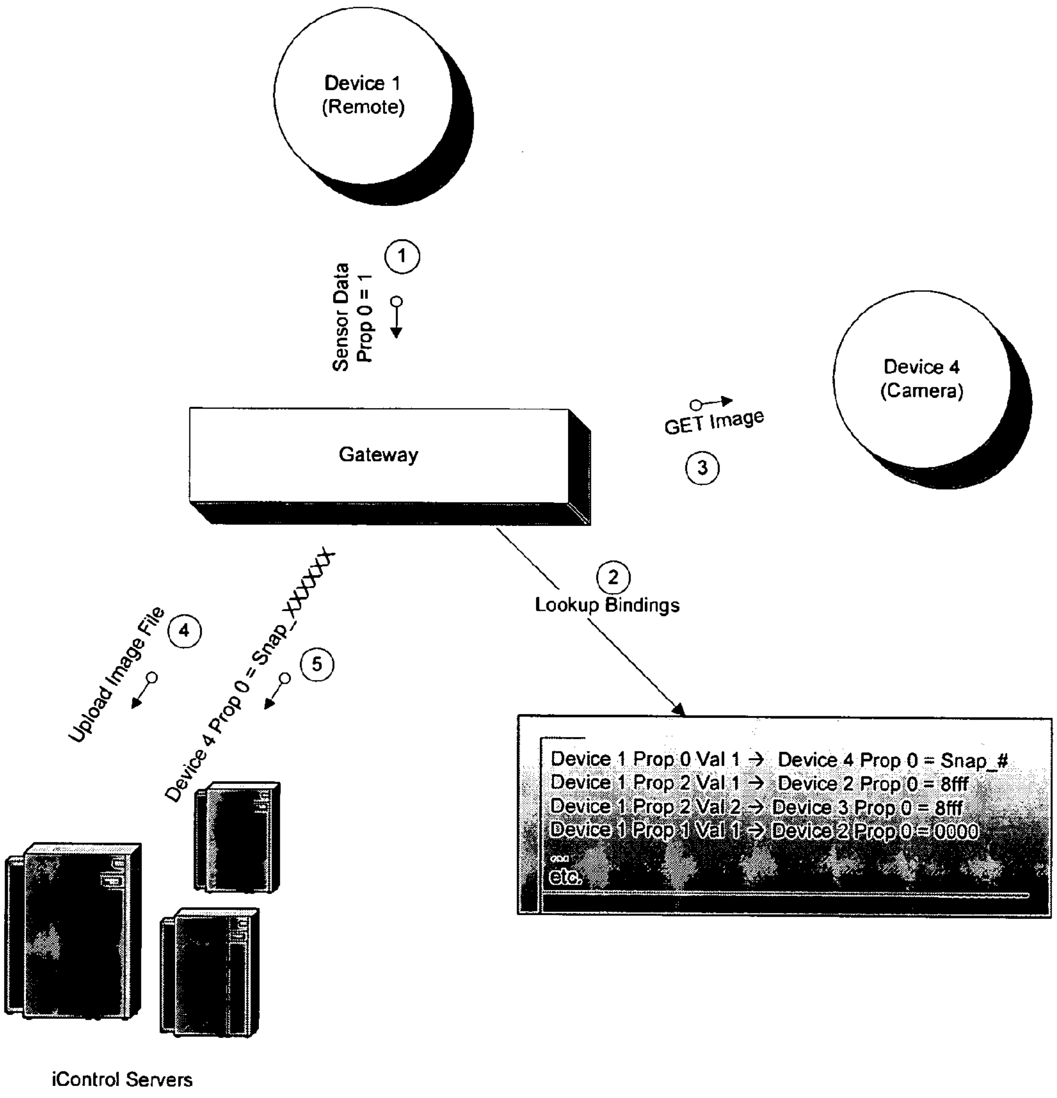

Device 1
(Remote)
1
Sensor Data
Prop 2 = 1
3
Sensor Data
Prop 2 = 2
5
Sensor Data
Prop 1 = 1
2
Actuator Data
Prop 0 = 8fff
Device 2
(Lamp 1)
5
Actuator Data
Prop 0 = 0000
Gateway
4
Actuator Data
Prop 0 = 8fff
Lookup Bindings
Device 3
(Lamp 2)
Device 1 Prop 2 Val 1 → Device 2 Prop 0 = 8fff
Device 1 Prop 2 Val 2 → Device 3 Prop 0 = 8fff
Device 1 Prop 1 Val 1 → Device 2 Prop 0 = 0000
etc.

Figure 10 - Binding Data Flow



Device 1
(Remote)
1
Sensor Data
Prop 0 = 1
Device 4
(Camera)
GET Image
3
Gateway
2
Lookup Bindings
Upload Image File
4
Device 4 Prop 0 = Snap_XXXXXX
5
Device 1 Prop 0 Val 1 → Device 4 Prop 0 = Snap_#
Device 1 Prop 2 Val 1 → Device 2 Prop 0 = 8fff
Device 1 Prop 2 Val 2 → Device 3 Prop 0 = 8fff
Device 1 Prop 1 Val 1 → Device 2 Prop 0 = 0000
etc.
iControl Servers

Figure 11

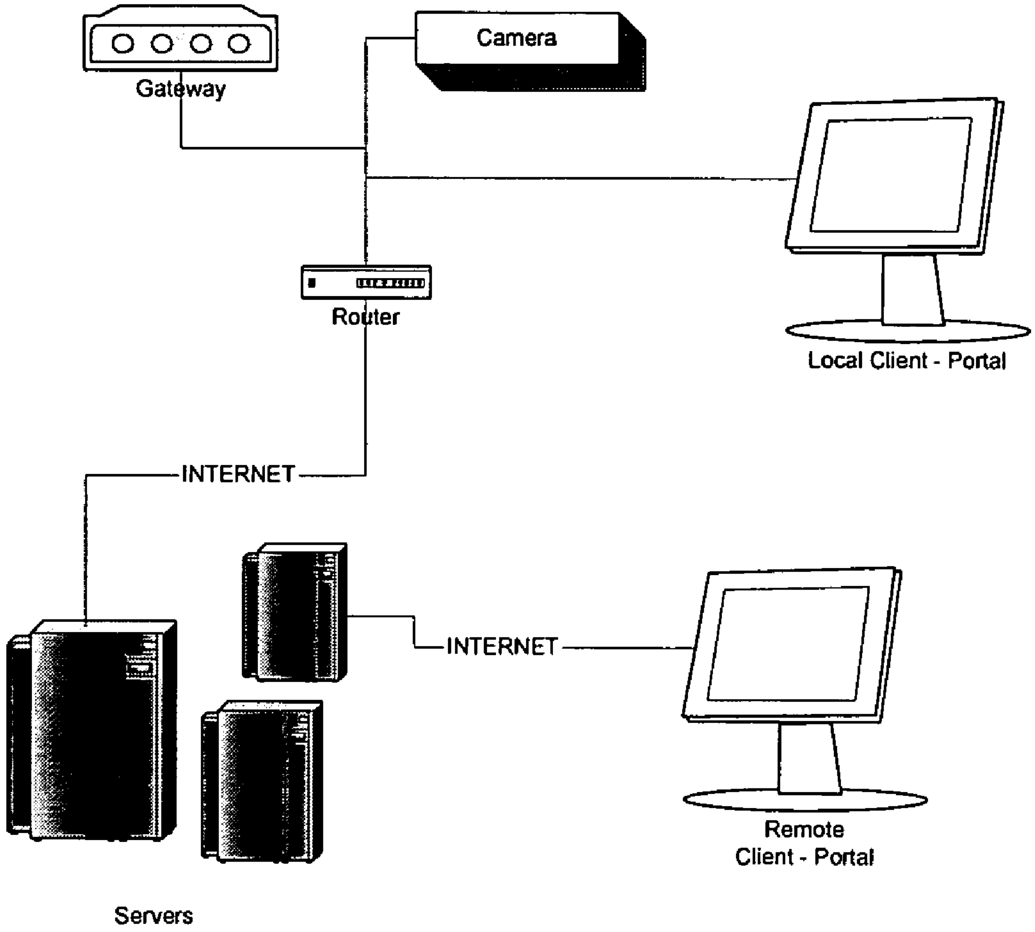

Camera
Gateway
Router
Local Client - Portal
INTERNET
INTERNET
Remote
Client - Portal
Servers

Figure 12 - Camera Image/Video Architecture

PREMISES MANAGEMENT NETWORKING

CROSS-REFERENCE

This application is related to and claims the benefit of the following United States patent applications:

U.S. provisional application No. 60/553,934 for Business Method for Premises Management, invented by Reza Raji and Chris Stevens, filed Mar. 16, 2004;

U.S. provisional application No. 60/553,932 for Premises Management Networking, invented by Gerry Gutt and Reza Raji, filed Mar. 16, 2004; and

U.S. provisional application No. 60/652,475 for Control Network, invented by Gerry Gutt and Reza Raji, filed Feb. 11, 2005.

Each of the foregoing applications is incorporated herein by reference in its entirety.

This application is also related to U.S. nonprovisional application entitled Business Method for Premises Management, invented by Reza Raji and Chris Stevens, being filed concurrently herewith, and which is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

Vendors such as premises vendors, communication service vendors, and Internet portal vendors need a solution for extending their relationship with vendees beyond the immediate transaction. Additionally, vendees desire additional premises management services beyond the immediate transaction for premises, communication services, or Internet portals. There is a need for advanced premises management services.

INCORPORATION BY REFERENCE

All publications and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication or patent application was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows an example of an overall network for premises management.

FIG. **2** shows an example of a homebuilder-branded Internet portal for premises management.

FIGS. **3**A-**3**C show examples of detailed screens of the portal interface for premises management.

FIG. **3**D shows a screen shot of a Internet Portal-branded portal for premises management according to an embodiment of the invention.

FIG. **3**E shows a screen shot of a main portal summary page according to an embodiment of the invention.

FIG. **3**F shows a screen shot of a portal showing details device information according to an embodiment of the invention.

FIG. **3**G shows an automation tab screen according to an embodiment of the invention.

FIG. **3**H shows a system tab screen according to an embodiment of the invention.

FIG. **4** is a diagram of a business method for premises management.

FIG. **5** is a diagram of a method for premises management networking.

FIG. **6** illustrates an example of a control network environment.

FIG. **7** is a block diagram of a control network with a gateway.

FIG. **8** is a flow diagram showing data being transformed, physically and logically, by a gateway.

FIG. **9** is a flow diagram showing the data conversion.

FIG. **10** is a diagram showing a gateway binding mechanism.

FIG. **11** is a diagram showing a camera snapshot scenario.

FIG. **12** is a diagram showing a camera environment.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** shows an example of an overall network for premises management. A premises **110** has premises management devices such as a smart thermostat **112**. The premises management devices are connected to a premises network **114** which can be, for example, an RF and/or power line network. The premises network **114** is connected to a gateway **116** which in turn is connected to a broadband device **119** such as a DSL, cable, or T1 line. The gateway **116** can alternatively or also be connected to a dial up modem **118**. The premises **110** is connected to the Internet **120**. The Internet **120** is connected to system managers at the network operations center **150**. The Internet **120** is also connected to customers of the system manager, for example vendors such as premises vendors, communication service vendors, or Internet portal vendors. The Internet **120** is also connected to vendees **140**, such as premises vendees, communication service vendees, or Internet portal vendees.

FIG. **2** shows an example of a homebuilder-branded Internet portal for premises management.

FIGS. **3**A-**3**H show examples of detailed screens of the portal interface for premises management. FIG. **3**A shows a main screen summarizing premises management services. FIG. **3**B shows a screen summarizing security management services and safety management services. FIG. **3**C shows a screen summarizing energy management services.

FIG. **3**D is another example, illustrating how services offered by the system can be branded and incorporated into a third part web portal, for example, in a personal portal such as one provided by Yahoo. The screen includes the usual Yahoo portal content such as the stock pane on the left, the news pane on the top and the calendar pane on the right. The system-specific pane is included on the bottom where the user can access monitoring and control information on the home or business. The look and feel of the system pane can be tailored by the service provider.

The system portal summary page in FIG. **3**E shows a snapshot of the state of the various devices in the user premises. At the top left is a drop-down box that displays the name of the premises being shown on the screen. The user can change premises by clicking on this box and selecting a different premises. A series of tabs allow the user to switch to Details, Notifications, Automation, Schedules and Systems screens for performing other system functions. The various panes on this page highlight different features.

The status pane lists the different devices in the user premises along with their actual states. The pending updates pane shows the time of the last communication between the premises and the server as well as any pending updates waiting to be sent downlink to the premises. The pictures pane shows the last several (e.g. last four) pictures taken by the camera in the user premises. The user can click on a thumbnail picture to look at a larger version of the photo as well as access archived images for that camera, look at live video, take new pictures or delete photos. The schedule pane shows the schedules activities for the premises. The alarm history shows an archive of the most recent event and activity in the user premises. The reminders pane provides a means for the system to remind the user to perform certain activities or functions related to their home or business. The mode drop down button on the blue navigation bar allows the user to switch between the systems modes. The QuikControl drop down allows the user to control any device that is controllable (e.g. camera, thermostat, lamps, etc.).

FIG. **3**F shows a details screen of the portal showing details device information. The details screen allows the user to show more detailed device data. The list on the left displays the system devices and their actual states/values. The pictures pane on the top right display the camera thumbnails (beyond the 4 displayed on the summary page). The thermostat pane on the bottom right shows the details of the thermostat data including the current temperature, cooling and heating set points as well as the thermostat mode.

FIG. **3**G shows an automation tab screen. This screen shows how the user may assign automation rules to devices such that an event caused by a device can trigger one or more actions by other devices. The left column shows all possible events that can occur based on the devices that belong to this premises network. The three columns, one per mode, identify the action for each event for that mode. For example, the figure shows that when hall motion sensor occupied event occurs in the away mode, the conference room camera takes a picture. The bottom portion of the screen shows that the wireless keychain remote control's buttons can also be programmed by the user to perform any action desired.

FIG. **3**H shows a system tab screen showing status of devices. The System screen shows a list of all the devices in the premises' network, including the gateway. Each device in the system is on a separate line. The first column shows the name of the device along with a status indicator which show different colors based on the status of the device (green for ok, yellow for offline, red for not found or problematic). There is also a "last update" column that displays the date and time of the last signal received from that device. The third column (device) describes the type and model number for that device. The user can get more detailed information about a device by clicking on the line corresponding to the respective device.

FIG. **4** is a diagram of a business method for premises management. In **410**, an Internet portal is available for access to a vendee, such as a premises vendee, communication service vendee, and/or an Internet portal vendee. In **420**, at least after a transaction between the vendor and the vendee, such as a premises transaction, a communication services transaction, and/or Internet portal services transaction, premises management services are provided via the Internet portal to the vendee. In **430**, the Internet portal is branded with the brand of the vendor. The shown steps can be added to, removed, rearranged, and/or modified.

FIG. **5** shows a diagram of a method for premises management networking. In **510**, premises management devices connected to a gateway at a premises are monitored. In **520**, premises management devices connected to the gateway at the premises are controlled. In **530**, an uplink-initiation signal associated with a network operations center server is received at the premises. In **540**, in response to the uplink-initiation signal, communications between the gateway and the network operations center server are initiated from the gateway at the premises. In **550**, during the communications between the gateway and the network operations center server, information associated with the premises management devices is communicated.

Property developers and service providers can:

1. Differentiate their offering from their competitors'
2. Generate new recurring revenue through new, value-added services
3. Reduce their operating costs
4. Increase the value of their offering
5. Increase the effectiveness and reach of their brand
6. Make smarter, knowledge-based business decisions
7. Increase customer retention and satisfaction

Additional content leverages the broadband infrastructure, thereby increasing the effective value of the broadband pipe.

Property developers/managers and service providers are facing ever increasing competition and lack the expertise, time and resources to offer control and telemetry services to their customers. Connecting people to devices is the next evolutionary step for the Internet.

Some of the architectural/design goals for the system are low cost, ease of use, and scalability.

The architecture and products/service offering is flexible enough to cater to the needs of the homeowner while being scalable and intuitive enough to allow for easy installation and minimal support.

Three types of customers are envisioned for the system. Although the ultimate end user is the property owner, customers can be: home developers and commercial property, e.g. multiple tenant unit (MTU) owners and managers; service providers (telcos, cable companies, ISPs, etc.); and homeowners or commercial building tenants.

The actual user of the services resides in the premises where, for example, the gateway and devices are installed. The system can be intuitive enough that the "average" end user can perform the installation and configuration steps.

The installer can be the person or entity that installs the gateway and the devices in the home, configures the gateway, connects the gateway to the Internet and/or telephone line and/or performs any troubleshooting necessary. Depending on the actual customer, the installer can be 1) the installation crew of the service provider or property developer, 2) an outsourced installation outfit hired by the service provider or property developer, 3) an outsourced installation outfit hired by the end user, or 4) the end user.

The premises gateway can be a low-cost and stand-alone unit that connects the in-premises devices to the server. The connectivity to the Internet can be accomplished via a broadband connection (T1, DSL or cable) and/or via the telephone line. Though broadband connectivity is preferred due to its persistence and throughput, telephone connectivity is recommended to be present as a back-up option in case the broadband connection is lost. For premises without a broadband connection (e.g., vacation homes) a telephone-only connection can be used.

The service portal provides an intuitive end user interface to the premises network as well as access to system and network configuration screens and user account information and settings.

Some embodiments of the overall system can be put in use through the following steps:

1. Customer need for telemetry services is established
2. Customer (via web or phone) orders a system
3. Customer acquires system (via service provider, builder, etc.)
4. A service account is established (by the service provider/builder or by the homeowner or system manager)
5. Gateway is registered (by the service provider/builder or by the homeowner)
6. Gateway sends network/device information to the server

7. Homeowner configures own home (alarms, notifications, binding, etc.)
8. Future devices are added to system either via pre-configuration by system manager or via the end user through configuration screens on portal

Each of these steps is described below:

Customer Need is Established

This can done through the property developer, the service provider sales channel or direct advertising by the system manager.

Customer Orders a System from System Manager

The customer specifies what kinds of devices are needed and where each one will reside in the premises (e.g., living room thermostat, lobby motion sensor, etc.). The user account is then appended by system manager to include this information as well as the actual unique ID for each device shipped to the customer.

Customer Acquires System

The gateway and devices can be acquired by the customer in several ways:

1. Pre-installed by the property builder/developer/manager or service provider
2. Directly purchased by the end user

The choice of devices can depend on the particular services and functionality desired by the customer.

Once the customer acquires the gateway and devices, the devices are physically installed in the premises. This task can be performed with the help of an installer, or for smaller premises, performed by the end user.

A Service Account is Established

This is generally done by the end user as the process uses personal information (name, payment option, etc.). The account registration involves the user logging on to the system manager web site and establishing a new account by entering name, address, phone number, payment details and/or the gateway serial number printed on the gateway in the end user's possession.

In some cases the system manager service account may already be pre-established with the gateway serial number and the end user simply has to update the account with personal and payment information. This scenario eliminates the need for the end user to deal with any cumbersome serial numbers or keys and is really more of a personalization step.

Multiple gateways can also be handled per user account.

Gateway is Registered

This step involves the association of the user account on the system manager server (established in the previous step) with an actual gateway in the user's home. The gateway is connected to a broadband network or the telephone line in the home.

For this step, the installer, for example, presses a SYNCH button on the gateway, and initiates an uplink communication from the gateway to the system manager server using a default (first-time) IP address or, in the case of a dial-up-only connection, a toll free number dial by the gateway.

Upon establishing a connection with the server and locating its corresponding user account (e.g., established in a prior step), the gateway acquires a system manager server IP address (to be used from that point on for all gateway to server communication), and changes its state from unregistered to registered.

In the case where the gateway is pre-installed by the developer or service provider, this step may have already been performed.

The gateway may not be able to perform any functions until it has gone through this registration process (as indicated by the state of the gateway).

Gateway Sends Network/Device Information to the Server

This is done on a regular basis and can always be initiated by the gateway. The server dictates the interval for uplink communication initiation between the gateway and server.

Homeowner cconfigures Home (Alarms, Notifications, Binding, etc.)

This is the normal use of the system manager portal whereby the user selects the various monitoring, logging and notification options.

Future Devices are Added to System

The end user obtains additional devices from the system manager, in which case they are added to the end user system by the system manager before being shipped to the customer.

Alternatively, the end user could purchase a device from a third party source in which case they could use the system manager portal interface to add (or replace) the device manually.

In addition, the system manager gateway can have a provision for "discovering" devices by listening for RF messages (e.g., GE Interlogix) or service pin messages (e.g., LonWorks devices).

Overview

Parts of the system as a whole are described, including the gateway, the server and the web portal interface.

System Overview

At the highest level, the system provides its users with a hosted and managed service for premises device monitoring and control for a fee, such as a monthly subscription fee. The premises markets include residential homes, commercial MTUs as well as small businesses.

The traditional complexity and expense of installing and maintaining such a system is delegated to the system manager platform. As a revenue-grade Application Service Provider (ASP) business, the system provides reliability, scalability, security, cost-effectiveness, ease-of-use, and flexibility.

The term "system" can denote the portal, server, gateway and end devices.

Reliability

The system can provide a high degree of reliability. This includes 24-7 operation of the Network Operations Center (NOC) and the server software it contains, and the reliability and fault-tolerance of the gateway and the control devices.

Scalability

The system, specifically the NOC, can scale to accommodate large Numbers (in one embodiment, millions) of gateways and devices (in one embodiment, tens of millions). Though this may not be used at the onset, necessary architectural provisions can be built into the system to allow for such expandability.

Security

As a revenue-grade service offering, the system provides security against intentional and unintentional interference with the normal operation of the system. The system can be reasonably immune to external unauthorized access (either over the Internet or device network media). The system can provide reasonable protection against spoofing (of NOC server, gateway or device).

Cost-Effectiveness

Similar systems in the past have suffered from a high cost of in-premises devices and gateway as well as high and/or unpredictable installation costs. The system installation process is simple in order to minimize, if not eliminate, the installation costs.

Ease-of-Use

The gateway and device installation process as well as the various user configuration and normal use menus/screens presented by the portal are, according to an embodiment, intuitive and easy to use. This eases the adoption and continued use of the system by its users.

Flexibility

The system is flexible enough to easily handle different device networking protocols/technologies should the need arise in the future. In addition, the system, including the web interface, can be adapted to different markets and applications.

Variable Logging

The system can log any device variable specified by the user for up to, for example, 30 days. The user defines a logging interval for each variable at the time of configuration. The logging feature can be handled by the gateway on the local device side and the data can be transferred to the server at regular intervals. The overall variable log for all variables can be kept on the server side.

Logging of data for more than, for example, 30 days (but no more than, for example, 180 days) can be provided to the user, for example for a nominal fee.

The system can allow for the logging of at least, for example, 10 variables per gateway. The minimum logging interval for any variable can be, for example, 5 minutes. Logging intervals provided can be, for example, 5, 15, 30, 60, 180 minutes as well as 6, 12, 24 hours and weekly.

Activity Logging and Tracking

The system must be able to provide at least, for example, a 14-day history log of all user, system and device actions. An action includes a change to a device variable, system or network settings brought on by either the system or the user (e.g., variable changed, logging enabled, device added, user notified, etc.). The user can trace back system activities to their cause and to the date and time they occurred. Past activities can be searched by variable, device, category or date.

System Modes

The system can support user-defined modes, such as "home", "away", "sleep", "vacation", etc. The mode the user network is in plays a factor in the determination of the actions taken (reporting, alarming, eventing, notification, etc.) by the system when variable changes occur.

System mode can be changed by the user via methods such as:

1. Via the portal interface
2. Through a schedule set by the user
3. Via a binding (a variable change tied to the mode change—e.g., RF remote control)

The system can provide a set of default modes based on the user profile (homeowner, business, vacation home, etc.). These default modes are a starting point that can be changed or added to by the user at any time.

Alarming

The user can specify alarm conditions for variables with discrete states (e.g., binary ON/OFF). These alarms can be reported in real-time (i.e., immediate uplink) by the gateway to the server. The server then in turn looks at the data and determines, based on user alarm settings, whether to notify the user or not.

Alarm conditions can be determined based on the value or state of a variable as well as the system mode.

Eventing

For non-critical events, the system can notify the user in non-real-time fashion regarding the state of any variable specified by the user. The variables chosen for user eventing can be of any kind (discrete or continuous). The gateway updates the server with the change of variable state/value at a regularly scheduled upload. The server continuously looks at variable data and determines, based on user eventing settings, whether to notify the user or not.

Eventing conditions can be determined based on the value or state of a variable as well as the system mode.

User Notification

The system can support user alarming and eventing via the following methods: email, text messaging, pager, and/or voice telephone call (voice synthesis).

Device Data Monitoring and Control

The user can specify any device variable for monitoring and control via the server portal. For example, up to 255 devices can be supported by a single gateway. For example, up to 512 variables can be supported by a single gateway.

The user can schedule specific variable updates (e.g., turn off thermostat at 8 am every Tuesday). Scheduled events can be canceled (gateway-server protocol can support this). A scheduled variable update is allowed, per time stamp and variable ID. If time stamp and variable ID match an existing scheduled variable change, then the value for that pending variable change is re-written with the new value. A given variable can have multiple scheduled values as long as each scheduled update has a different time stamp.

Any pending downlink variable change commands can be canceled that have not been relayed to the gateway at any time through the portal interface.

Device Network Support

The system can support an open architecture where most, if not all device networking protocols can be supported. Examples of specific device protocols supported by the system include RF and powerline protocols, such as GE Interlogix RF and Echelon LonWorks power line (PL & FT), simplifying the installation burden by requiring no new wires to be installed in a premises.

The LonWorks free topology twisted pair medium (FT-10) can be supported as an option to better support commercial applications (e.g., office buildings).

All devices, regardless of the technology, can possess these attributes:

1. Unique ID (global)
2. Non-volatility. Must not lose any pertinent data or state.
3. Low-battery indication over the network (if battery-operated)
4. Tamper detection (if security-sensitive)

RF

This system includes a low-level, simple unidirectional protocol for multiple sensors to talk to a receiver head end. The protocol needs and footprint are relatively small and as such the RF devices are comparatively low-cost and small. They also can function for several years without the need for a battery change for simplified installation and maintenance of the system by the user.

A bi-directional RF transceiver can be supported by the system. This allows for control as well as monitoring of remote devices (e.g., thermostat) by the user.

The following RF devices can be supported by the system:

1. Door and windows sensor
2. Motion sensor
3. Smoke alarm
4. Water sensor
5. Freeze sensor
6. Contact closure sensor (e.g., ITI DWS with external connector pins)
7. CO alarm
8. Heat sensor
9. Thermostat
10. RF remote control

PL

The power line solution offers a robust and reliable mechanism for communicating over existing residential power line wiring.

The following PL devices can be supported by the system:

1. Thermostat (e.g., RCS)
2. Load controller (e.g., Halen Smart)
3. Relay actuator (e.g., Comap)
4. Photo camera, e.g., black & white, low-resolution (with motion sensor)

FT

The Free Topology solution offers a cost-effective medium for commercial applications. Many third party LonWorks devices use this medium for communications.

Other Devices

The following is a non-exhaustive list of a few other devices supported by the system.

1. Small data/message display—for text messages, news, weather, stock, photos, etc.
2. Door latch control
3. Pool/spa controller
4. Weather station
5. Lighting control
6. Elderly or disabled monitoring
7. Irrigation controller (Bibija)
8. VCR programming

Cameras

The system can support cameras. For example, standard off-the-shelf IP cameras (also referred to as web cameras) may be used, such as those available from vendors such as Axis, Panasonic, Veo, D-Link, and Linksys, or other cameras manufactured for remote surveillance and monitoring.

Surveillance cameras may contain a standalone web server and a unique IP address may be assigned to the camera. The user of such a camera would typically retrieve the camera image by accessing the camera's web page through a standard web browser, using the camera's IP address. In some cases the IP camera acquires a local IP address by using a DHCP client to negotiate an address from the local DHCP server (usually residing in the user's router/firewall).

According to an embodiment, the gateway treats camera images as it does other sensor or device data. User commands to "snap" a picture are sent from the system's portal/server to the local premises gateway during scheduled communications between the gateway and server (initiated by the gateway). Alternatively, a picture "snap" command for a local or remote camera can be initiated by a sensor (e.g., motion detector, remote control, etc.) on the local device network. The gateway then in turn talks to the camera over the IP network (wired or wireless) to retrieve the image and pass that image up to the system's backend server, effectively acting as a pass-through agent for the camera.

Since the data from the gateway (including the camera image) is pushed up from the gateway to the server using standard HTTP protocol (used by web browsers), additional configuration of the user network may be avoided. Also, adjusting of the user's firewall (port forwarding, DMZ, etc.) may be avoided (i.e., simpler installation and enhanced security).

Also, the push mechanism eliminates all the issues related to accessing the camera from the Internet, namely firewall and dynamic IP issues mentioned above, since the user gets the images from the system servers and not from the premises directly.

The system's user portal interface acts as a unified user interface for the user by displaying multiple images from different cameras in the same user interface page (e.g., web page).

The system's IP cameras can be physically located anywhere as long as they are connected to the Internet (if remote) or to the local IP network (if local).

Due to the fact that the images are served from the system's server (as opposed to the local camera or network) potential security exposure of accessing the home network directly from the outside may be avoided. Also, additional security measures can be put in place (e.g., SSL) to block an unauthorized user from accessing the images on the server.

Device Low-Battery Notification

The system can notify the user via the web portal of any low-battery conditions for the devices that operate on battery (e.g., GE Interlogix devices).

Server-Side Binding

The system can send variable control information downlink based on variable information collected through the uplink connection. This rule-based exchange can take place within the same atomic uplink-downlink (request-response) exchange between the gateway and server. The user specifies the actual "rules" for such bindings (e.g., turn off the thermostat when there is no motion in the premises for 2 hours).

This implementation may impact scalability because of the atomic communication factor.

Local Binding

Local binding can permit a more real-time interaction between devices. This functionality can take place without the server's involvement (other than the initial configuration of the local rules). The local binding, given the different technologies used at the device level, needs to be routed through the gateway.

Gateway Shoulder Tap

The server can "call" a gateway if the user requests that a variable change be propagated to a device in real-time (rather than waiting for the next gateway uplink connection on).

Device Sharing Between Different Users

The system can provide a means for a single device to be managed by multiple users. For example, a security gate or a pool temperature sensor in a property common area should be accessible by all residents in the complex.

Gateway

The gateway is the central link between the premises device network and the backend server. It can be a thin, low-cost client of the server and use the least amount of hardware and software without compromising the basic functionality and objectives of the overall system.

Internet Connectivity

The gateway can provide both a connection to a broadband network (Ethernet DSL or cable modem) and telephone network. The telephone network connection provides a second, redundant route for accessing the server in case the broadband network access is down and there is a need for the gateway to report critical alarm information uplink to the server. The telephone connection also provides a means for the system to support premises that have no broadband connection available (e.g., as in many second or vacation homes).

The gateway can terminate any data call in process if a user picks up a telephone and provide a dial tone immediately. In addition, the gateway may not initiate a data call if the phone is in use by the user (off hook).

They gateway can dial out in the absence of external power to the gateway.

Communication with Server

The gateway can initiate all communications with the server. Gateway communication can either initiate based on a predetermined schedule (e.g., every 30 minutes) or due to a local premises alarm (selected by the user).

Gateways can contact a common server for their first uplink connection in order to obtain their assigned gateway server address, which they can use for all subsequent uplink connections (unless changed later by the system). In the event that the gateway cannot connect to its designated gateway server, it can fall back to contacting the default initial gateway in order to refresh its gateway server address.

The predetermined call initiation schedule can be programmable by the server and can provide different intervals for broadband and telephone intervals (e.g., every 30 minutes for broadband and every 90 minutes for telephone).

By assigning the gateway-server communication initiation to the gateway the system can enjoy the following benefits:

1. Most if not all issues generally attributed to routers, firewalls and NAT are eliminated, as the gateway is now simply an HTTP client (much like a web browser).

2. Security against outside hackers is greatly increased as access into the gateway can be disallowed. The gateway knows whom it can talk to (server) and it does so when it needs to.

A possible disadvantage of a push-only scheme can be an inability of the server to provide "real-time" device control. This can be a relatively minor disadvantage minimized through the shoulder-tap mechanism.

Gateway Shoulder Tap

The gateway can have the provision of initiating an uplink communication based on a telephone ring signal detected on the phone line. This shoulder tap from the server allows the server to pass down a variable change to the gateway without having to wait for the next gateway uplink connection.

A drawback of a telephone line shoulder tap is the occasional ringing on the telephone line. It is difficult to detect an incoming ring reliably without the phone actually ringing. This is fairly benign when considering:

1. Most user variable change requests (control) may not have to be done in real-time and can occur at the next scheduled gateway uplink synch.

2. Most often the premises (e.g., home) being controlled in real-time is unoccupied.

3. The shoulder tap can at most ring the phone only once so the user can wait for the second ring before picking up the phone

4. The user can opt to provide a second phone line dedicated to the gateway.

Implementing shoulder tap over IP is another embodiment with a more complicated installation process (e.g., router/firewall configuration, opening ports, etc.). Keeping an IP connection alive between the gateway and server can be unreliable and could heavily burden the server.

Configuration

The gateway can be installed without any special skills. The NOC server can handle the complexity of configuration.

Once plugged into a power outlet as well as a broadband and/or telephone network, the gateway can:

1. Determine if there is a broadband connection available

2. If so, obtain an address from the local DHCP server

3. Make sure the telephone connection is operational

4. Contact the server for the first time and check to see if there is a user account associated with it (this can be a secured inquiry to eliminate hacking)

5. If there is no associated user account found, notify the user (e.g., blinking LED on front panel)

Device Discovery

The gateway can be put into a device discovery mode via, for example, a front panel push button. Devices can normally be introduced to the system and assigned to the user:

1. By system manager before shipping out to the user

2. By the user/installer via the portal device registration screens

The discovery mode is a third way of registering devices. The discovery mode allows the gateway to listen for and discover new devices added to the network—should there ever be a need for such functionality. Upon discovery of a new device the information is passed to the server for further processing and registration. The user can then finalize the device registration process through the system's portal (e.g., assigning names, alarming, etc.).

If the user can specify the adding of a device, it can be configured by the user immediately on the portal. Auto-configuration comes with set defaults. Another similar device to copy can be specified.

Auto Recovery

The gateway can be self-sustaining and autonomous.

In the event of communication failure between the gateway and the server for an extended period of time the gateway can continue to do its tasks (e.g., variable monitoring, logging, etc.).

In the event of an extended power loss or a system reset, the gateway can resume normal operation after the appropriate "boot-up" period (i.e., no more than 2-3 minutes). A hardware buffer can receive, e.g., RF signals during bootup.

Any pending scheduled events that did not occur because of the power loss can be performed once the gateway has resumed normal operation and can occur in the original order defined by the user.

In the event that the gateway software "hangs," the gateway can recover itself through a built-in watchdog-monitoring feature.

Rule-Based "Binding"

Gateway Power Interruption

The gateway can operate for at least, e.g., 5 minutes after a power failure in order to report its latest status (including the power status) to the server (either via broadband or telephone). The gateway may not use a rechargeable battery in order to eliminate the need for gateway servicing when the battery reaches the need of its life (e.g., typically 2-3 years).

The gateway can withstand power interruptions without losing any pertinent data (e.g., device data, log data, date & time).

For applications where the gateway and devices are to operate in the absence of power, the user can obtain and use an uninterruptible power supply (UPS).

Remote Firmware Upgrade

The gateway can receive firmware upgrades over its WAN connection (Internet or PSTN). The gateway can have provision for recovery in case there is an interruption during a firmware download (e.g., network connection loss).

The gateway firmware upgrade is an automated process initiated by the gateway based on a schedule downloaded from the server during a gateway-server exchange. The upgrade process may not involve any user interaction or involvement and may take place when the user is least likely to be using the system (e.g., at night).

Variable Logging

The gateway can provide enough storage for logging one day worth of data for, e.g., 10 variables logged every, e.g., 15 minutes. In the event that the local gateway log is filled up before the gateway has had a chance to upload the data to the gateway, the gateway can stop logging additional data and report a "log full" error to the server at the next uplink connection.

Security

Appropriate security measures can be provided by the gateway to ensure protection against:

1. Inadvertent communication with neighboring networks and device's not related to a gateway/user.

2. Intentional external hacking into the system from the WAN side (Internet and PSTN).

3. Intentional external hacking in to the device network side (PL or RF).

Power Consumption

The gateway can use minimal operating power in order to reduce the cost associated with the power supply as well as the circuitry to keep the gateway alive immediately after a power failure.

Form Factor

The gateway can be encased in a visually attractive enclosure that is generic enough for multiple markets including consumer applications and commercial building applications (schools, etc.).

Ease of Use

The gateway can use the simplest possible installation procedure. The gateway can "figure out" how to communicate with the NOC (broadband and/or PSTN) once the power has been connected to it. No user involvement may be necessary for this to take place.

User Interface

The gateway's user interfaces include the following LEDs and switches:

POWER LED

COMM LED: communication happening between gateway and server

DEVICE LED: Device communication (PL or RF) happening. This LED can also be used for the device discovery feature.

ERROR LED: Displays different errors using different blink rates (log error, synch error, comm. error)

SYNCH switch: Initiates a gateway-server uplink communication

Gateway Local Reset

The gateway can provide a way for it to be reset locally by the user. Upon the execution of this gateway reset function, the gateway can be in the factory default state with no device, variable, user or configuration variables residing in it.

The reset operation for the gateway can be performed by, e.g., holding down the SYNCH switch for 20 seconds.

Agency Certifications

The gateway can be designed to comply with both FCC Part 15 (Level B) and Part 68 certifications.

If an external Tamura power supply is not used, then gateway design can meet the standards for the appropriate regional safety agency certification (i.e., UL, CSA, CE, and TUV).

Error Reporting

The system can report error to the user and/or administrator when the following conditions occur:

1. Downlink variable update failed
2. Gateway synch delayed or missed
3. Missing variable poll value
4. Variable log full
5. Broadband or phone line connection down

Server

The server provides a hosted, reliable and secure "server-in-the-sky" for the premises gateways to communicate to and for the users (customers) to access for accessing and controlling the various devices in one or more premises.

Reliability

The NOC facility can be run by a managed hosting service and as such provisions for power failure and security (theft) can be in place via the vendor providing the hosting service. However, the NOC server software architecture can support certain backup features.

All user, system, network, gateway and device data contained by the NOC server can be backed up on a regular schedule (e.g., once a day).

When NOC server hardware malfunctions, that hardware can be quickly and easily replaced with minimum user downtime.

Security

The server can communicate to the gateway in a secure fashion.

The data can be encrypted when transferring between the gateway and server, as well as ID/password for authentication.

Scalability

The server software can be scalable such that it can support a large number of gateways over time. The scalability sold also enables the server to have a small foot print at the beginning when the number of gateways may be relatively small.

Platform

The interfaces between the servers and modules can be in XML in order to provide maximum flexibility and scalability. No requirements may be imposed for the operating system or programming language platforms used.

Server API

The server can provide an API (via XML and SOAP) that permits third party applications to get full access to the functionality of the server.

Portal

The portal can support web, WAP and PDA access points. An important attribute of the portal is ease-of-use.

Customization

The portal can present an automatically-customized UI to the user based on the application (e.g., residential, commercial, etc.) and the devices used (e.g., security, energy, safety, etc.).

As a secondary feature the portal can also allow the user to easily customize their portal for their particular needs.

Lastly, system manager personnel or authorized agents can further customize a portal for a specific customer (e.g., a telecom) or class of customers (e.g., homeowners of a home builder). This process can put a specific "skin" on a customer portal.

User Account Screens

These screens allow the end user to open an account and register the end user's gateway(s). Screens can be included for obtaining billing/payment info and other user information (e.g., address, primary contact information, phone number, etc.).

In addition, this can be where the user enters their gateway ID(s) (on the gateways) so the system can make an association between the logical user account and the physical user network(s)/gateway(s).

User notification options (email, phone, page, text messaging, etc.), as well as time zone, uplink interval can also be selected here.

The option to customize the WAP portal interface can be provided so the user can select the variables and the functionalities that are presented on a WAP device accessing the service.

Device Registration Screen

The user can register devices obtained from other sources-assuming they were not pre-registered already by the system manager. The user can enter the unique device ID and the device name, etc.

The ability to delete a device from the local user network can be provided. History related to the device being deleted (log data, action tracking, etc.) can be removed from the system, e.g., 30 days after the device deletion.

The gateway can know if something succeeds or not and report it back to the server. Similarly, each "command" the server performs on the gateway can be tracked back when the results of what the gateway did with it come back (e.g., success, fail, etc.).

The gateway can report the downlink changes like it reports uplink changes. The state change of the variable in question (e.g., Change thermostat setpoint) can appear in the log like any other variable, along with its time stamp.

The portal can set the change, then after the change occurs it can verify it is reported in the log. For example, if the portal is asked to turn the light on, it can be ensured that it happened "once and only once" and if it failed, that can be known.

The ability to replace a device in the local user network can also be provided. Old log data for the replaced device can be kept without a break in the device's data (i.e., the log can start getting values from the new device. Also, since the downlink values are set on the new device, those initial settings can also appear in the log.

Network Configuration Screens

This is where the user configures the device network and sets preferences and options (e.g., which variables to monitor, logging options, etc.).

Provisions for creating variable groupings are also provided here (i.e., defining a single variable that represents the collection of all similar type variables selected by the user—either ANY or ALL function (OR or AND)—e.g., all door/windows sensor states).

The user selection of which variables are monitored for eventing and alarming is performed here as well.

Normal Usage Screens

These represent the main screens used most often by the user on a day-to-day basis. Typical functionality provided includes: network summary, variable monitoring, variable control, variable logging, system activity log, system status, alarms, etc.

WAP Interface

The portal can also provide a simplified interface for supporting WAP devices. The functionality can be a limited subset of monitoring and control services offered by the web portal.

The customization of the WAP portal interface can be done through the normal Web interface screens

PDA interface

The portal can also provide a simplified interface for supporting browsers running on PDAs. The functionality can be a limited subset of monitoring and control services offered by the web portal.

The customization of the PDA portal interface can be done through the normal Web interface screens (see above).

Permission Levels

The portal, in association with the server, can provide configurable user access and permission levels for both inter-account (e.g., different premises) and intra-account (e.g., mom, dad & kid) isolation.

Other Features

1. A desktop application in the icon tray that reports alarms and events in the background.

2. Support for larger premises (single user with multiple gateways)

3. Support for multiple users/locations per gateway

4. Rule-based local binding

5. IPSec (e.g., via HiFn chips)

6. Support for LonWorks free topology (FT-10) devices by the gateway

Control Network

An embodiment of a control network may comprise a collection of sensor and actuator devices that are networked together.

Sensor devices are devices that sense something about their surroundings and report what they sense on the network. Examples of sensor devices are door/window sensors, motion detectors, smoke detectors and remote controls.

Actuator devices are devices that receive commands over the network and then perform some physical action. Actuator devices may include light dimmers, appliance controllers,-burglar alarm sirens and cameras. Some actuator devices also act as sensors, in that after they respond to a command, the result of that command is sent back over the network. For example, a light dimmer may return the value that it was set to. A camera returns an image after has been commanded to snap a picture.

The core of an embodiment of a control network is an architecture where sensor devices are coupled to actuator devices. A light switch, for example, may turn on a lamp through a light dimmer actuator. A door/window sensor or smoke detector triggers an alarm. Other devices may also be controlled in various ways.

FIG. 6 illustrates an example of a control network environment. Here three different networks with devices are depicted (GE security, LonWorks, IP). The LonWorks network includes a light switch and lamp, the GE network has some door sensors and an alarm controller, and the IP network has some IP cameras attached.

Note that the computer in the middle of the network may be used to bridge the various networks, essentially providing interoperability, but with available existing technologies that calls for a custom solution requiring expensive custom software. Otherwise, the three control networks are independent.

FIG. 7 depicts one embodiment of an architecture that uses these described concepts.

Here we see the same three local networks on the premises (IP, LonWorks, GE Security). However, now they are all connected together by the system gateway. Furthermore, the system gateway is attached to the internet, through which it regularly contacts the system servers in order to send up new data and get back control and configuration information. Clients can monitor and control their premises using ordinary browsers on a wide variety of devices by accessing the system servers.

Note that, at the premises, use of a PC or custom programming to achieve interoperability between different device technologies, or to provide remote monitoring and control may be avoided. Instead, in an embodiment both functions are performed by the system gateway, which according to an embodiment is designed to interface to a variety of device technologies and provide an abstraction layer that helps the rest of the system (servers and clients) to be technology-neutral.

Sensor/Actuator Device Abstraction

Sensor and actuator devices are abstracted at the gateway hardware level so that different devices from different manufacturers can be handled seamlessly. Embodiments may support devices from several different manufacturers (for example, GE Security, Axis Communications, Axsys Systems) using three different communications technologies (unlicensed-band RF for GE devices, Internet Protocol for IP cameras, and powerline for LonWorks modules).

Gateway Device

The gateway device performs the hardware abstraction function according to an embodiment of the invention. The gateway includes the hardware and software required to communicate with all supported device technologies. Software on the gateway converts the raw data received from the device to an indexed data point. Periodically the gateway sends the data to the server, with each datum tagged with its data point index and time stamp.

In an embodiment, the server performs substantial operations for data storage and user interface.

Gateway—Server Data Interface

Between the server and the gateway, an embodiment of the system uses a device-property-value model. Each device supports some number of properties that expose its capabilities. For example, an embodiment of a door sensor has a state property (open or close) and a battery-level property (low or ok). Both the devices and their properties are given indexes when the gateway is configured, and all subsequent data exchange uses the indexes to identify the property involved. This indexed property ID may also be referred to as an "indexed data point."

FIG. **8** illustrates how data is transformed, physically and logically, by the gateway.

The door sensor has detected an open door, and sends the gateway a message with its hardware ID and raw value. The gateway interprets the data, converts it to an indexed data point value, and sends it to the server as device #**1**, property #**0**, set to 1 (true). Note that the device ID is converted to the configured device index (1), and the changed property is identified by its property index (0).

In the second case, the client wants to take a picture, so the server sends down the value (in this case, the desired picture name) indexed by the camera's device index (2) and the camera's picture property's index (1). In this case, the gateway initiates a web service to the camera to access (and upload) the image, then sends back the result of that operation to the server, again as an indexed data point.

According to an embodiment, the camera and a door sensor are both handled identically by the server and in the server-gateway protocol, using the device+property model.

Common Device Definition Format

In the server infrastructure, the device data is handled as indexed data point values. When the data is presented to the user, it is reinterpreted. The device definition file is the mechanism that permits the server software to handle this reinterpretation with a single, common code module, independent of device types or technologies.

Physical devices are defined using a common device definition file format which provides the information necessary to convert the device- and technology-specific view of a device to an abstracted, generalized view.

Function Types and Properties Abstraction

In order to allow client inspection and manipulation of sensor/actuator devices in a device- and technology-independent manner, device capabilities are mapped to standard function types, each of which defines one or more standard properties. This permits client software to, for example, query the system for temperature measurements, without necessarily knowing what physical device type provided it or what networking technology it used.

Raw Data Types

Each property in a device definition is tagged with its raw data type. This is the format of the raw data as received from the device and passed up by the gateway. Note that this is usually not the same format as the raw data that is passed from the device to the gateway.

For Boolean (digital) properties, this raw value is either the string "1" or the string "0." For analog properties, the format of the value can vary widely depending on the type of device. The gateway does not have to be responsible for handling the wide variety of formats possible, since the raw format type is stored in the device type definition, and is used by the server to make the conversion when necessary.

Standard Data Types

Each property in the device definition file is further tagged with a standard data type. This is the type that is stored in the server database and, by default, reported to the client. (Note that the actual database field type is a string: the "standard type", as used here, refers to how that string is formatted, not to the database data type).

Formatter Conversion Classes

The server has a set of formatter classes that convert between the raw and standard formats. These are selected and instantiated dynamically, as needed, based on the raw and standard data type strings from the device definition. This way the server code that manages data is identical for all data types, and supporting a new data type includes creation of a new formatter conversion class. Similarly, there are a set of formatter classes that convert between different standard formats.

Data Conversion Data Flow

FIG. **9** illustrates how the data conversion is handled. Raw data is sent up by the gateway. The server uses the device definition to determine which raw data converter to invoke, calls the converter, and stores the standard data in the database. Later, when the data is read, the server accesses the standard data from the database, optionally reformats it to the client's specifications, then returns the formatted value to the client.

Associative Binding

Binding is the process of "connecting" the output of one device (a sensor) to another device (actuator). An example is a switch that triggers a light to go on.

Gateway Binding

First, whether the devices in question use the same technology or not, associative binding uses the gateway itself as the "connection" mechanism. The gateway receives the signals from the sensor, interprets them, and relays the appropriate message to the actuator.

Gateway binding can be implemented without associative binding. That may, however, involve the gateway containing code to do the data conversion from the source device's data format to the destination device's data format. For example, if a switch is bound to a lamp controller, switching the switch to on causes the lamp to turn on.

Associative Binding

The gateway implements a form of associative binding, where a binding (connection) is triggered by the value of a source device property. Bindings are kept in a table that maps source device properties+values to destination device properties+values. For example, consider a remote control that sends out a numeric value (for example, 1 to 10). Binding entries can map the individual values to different target devices, so that each value can turn on a different lamp. Furthermore, the binding entries contain the specific values that need to be sent to the target device property.

Each associative binding defined on the gateway may include:

Index of the source device property
Index of the target device property
Source property value
Destination property value

When a sensor's bound data point reports a change, the gateway checks whether there are any bindings that match that data value. If there are, it sends the appropriate destination data to the destination device property, hence to the destination device hardware.

FIG. **10** illustrates a gateway binding mechanism. The steps illustrated in the diagram are:

1. User presses on-1 button, remote sends "prop **2**=1"
2. Gateway finds "prop**2**=1" in table, sends "prop **0**=8fff" to Device **2** prop **0**
3. User presses on-2 button, remote sends "prop **2**=2"
4. Gateway finds "prop**2**=2" in table, sends "prop **0**=8fff" to Device **3** prop **0**
5. User presses off-1 button, remote sends "prop **1**=1"
6. Gateway finds "prop**1**=1" in table, sends "prop **0**=0000" to Device **2** prop **0**

Gateway Data Abstraction

The source and destination data are specified in the table as untyped strings, so the gateway can do a string comparison, which may not involve knowledge of the data semantics. The gateway passes the destination string back to the destination device, again without necessarily using semantic knowledge.

User Data Abstraction

In an embodiment of the system, the user knows the semantics of the data, but may not know the raw data formats. So the user knows that "when I press the lamp on button on my remote, I want the lamp to go to full brightness." Because the data from both the sensor and the actuator involved in a binding is normalized to standard data units, the user can specify their desired bindings using those standard data formats, and the system receives these selections. (In the above case, Remote "lamp" button="On" causes the Lamp to be set to "100%").

Server Data Abstraction

As in cases where the server handles sensor/actuator data, it does so in the case of bindings using the format conversion classes, driven by the device definition files. The server does not necessarily use semantic knowledge of the values being bound.

Gateway Device Abstraction

For a given user premises, in addition to the sensor and actuator data, there is system-level data that is managed. Some examples are error logs, usage logs, gateway error alerts, tracking changes to the system, etc. The gateway may be treated as a pseudo device.

In this design, system data are reported as properties belonging to the gateway pseudo device. Because the system properties are exposed this way, they can be transparently handled by the server infrastructure (logging, reporting, etc.) rather than requiring a separate logging/reporting mechanism. This enhances the resiliency of the server design, since new system properties can be added without changing the server code (simply adding the new system variables to the gateway device model suffices).

Camera Snapshot: Abstracting Images through Properties

The data from cameras (i.e., "camera" function types) is a relatively large binary file. An embodiment of this does not fit the simple property-value model, and in an embodiment the image is not represented by a string. An embodiment handles the cameras and camera properties like other devices where it is appropriate, yet still offers the camera features (still images and video) to the user. An embodiment does that by creating special properties for the camera.

Cameras contain a property named "snapshot" that is linked to the camera's images. This property performs: 1) writing to this property causes the camera to take a snapshot and upload it to the server, and 2) the property is logged when the property changes. The value of the property is the name of the snapshot image. That is used by the server to fetch an image given a name.

Taking a Snapshot

Clients write a string value to the snapshot property that gets sent down to the gateway. That causes the camera code in the gateway to get the snapshot from the camera and upload it to the server. Finally, it reports (to the server) that the property was successfully updated. While the gateway does require special code to handle the camera interface, the device property data is handled exactly like any other device property. FIG. **11** illustrates a camera snapshot scenario.

Logging Images

By using a regular property to represent an image snapshot, the times, names, etc. of the snapshots can be logged using the ordinary property logging mechanisms used for other properties. The client software uses this history log to display thumbnails of the saved images. As in the case of the server, the client software does not need special code to get the list of images (although it does use special code to display the thumbnails and images according to an embodiment).

Binding Snapshots

Because a snapshot is triggered by a property assignment, that assignment can also occur due to a binding. Thus combining this snapshot property functionality with the associative binding capability leads to a way to take snapshots based on reported sensor data.

FIG. **11** illustrates a camera snapshot binding mechanism. The steps depicted are:

1. User presses "take picture" button on remote, remote sends "Device **1** Prop **0**=1"
2. Gateway finds the binding in the table (Dev **4** Prop **0**=Snap_#)
3. The # at the end tells the camera code to append a random number
4. Gateway camera code gets the data update, initiates an HTTP GET to the camera
5. Gateway camera code sends the image to the server
6. Gateway reports updated data like any other data update.

Camera Integration

Embodiments of the server and gateway incorporate a number of features that simplify the installation and use of still and video cameras.

Camera Type Abstraction

As is the case for attached devices, cameras are abstracted on the gateway so that neither the client nor the server infrastructure necessarily has specific knowledge of the camera type, thus they may handle all cameras identically according to an embodiment. (Note: the client application—in our case the portal—may use some specific camera knowledge in order to present the video and stills transparently to the user).

Integrated Stills and Video

The camera stills and video are integrated into the user interface so that the user never sees any camera-specific web pages. FIG. **12** illustrates a camera environment.

Firewall-Proof Still Images

According to an embodiment, the images from the IP-attached cameras supported are not viewed from beyond the user's own local network unless the user's router opens a port and forwards the camera requests to the camera. However, since the gateway is behind the same firewall as the camera, it gets the image from the camera and transfers it to the server via HTTP port **80** (which is always open). The images thus become available to the user on the Internet (protected by username/password).

Integrated Video Dynamic DNS Replacement

Viewing video from the camera involves the client changing router settings to forward TCP requests to their camera. Then, the portal allows the client to access the video without the client necessarily knowing the Internet address of the client's system. The gateway is in regular communication with the server, and upon update the server saves the gateway's current WAN address. When the client wants to see video from the client's camera, the server inserts the gateway's WAN address into the video image link (href). If the user's IP address changes frequently, the user can access their camera's video from anywhere.

Installation

Network cameras on the market come with a variety of installation methods. An embodiment of the gateway eliminates the need for client involvement by automatically configuring the camera hardware.

During the camera configuration, the gateway creates private administrator password, then a view-only user with a random password that is subsequently used to get camera images (still or video). The gateway searches for the camera on the local network to obtain its IP address (as assigned by the user's router). Since the gateway itself is automatically configured via DHCP, it knows the subnet and approximate address range that the router is using for the DHCP-assigned addresses.

Configuration

According to an embodiment, the camera configuration capability is exposed via camera configuration properties. Should the user want to change the camera's address or client user name/password, the user can do so in one place, on the system portal. The changes are passed down to the gateway (as camera configuration property updates) where it causes the gateway to reconfigure the camera hardware. Differences between different camera types are handled by the gateway software. These properties are handled and logged as other properties.

Router Port Forwarding Assistance

Setting a router's port forwarding table to support remote video viewing may involve:

1. Determine that port forwarding is called for
2. Find the router's configuration web page
3. Figure out what to enter as the server address
4. Figure out what to enter as the server port
5. Know what to put where
6. Know if it is working correctly

An embodiment of the system addresses these items. Note that the user is logged on from the user's own network (the "Local Client" example in FIG. **12**) to configure the user's router.

Determining Port Forwarding is Desired

When the user accesses a camera from the system portal, the system server performs a test to check whether the camera is accessible from the Internet. If it is, the camera page includes a link to a page that will display the video. If the camera is not accessible, the video link instead opens a camera assistance page that guides the user through steps to configure their router's port forwarding.

Finding the Router's Web Page

Since the gateway is on the same internal network as the camera, it knows what the router's address is (it is the default gateway passed back in the DHCP assignment). The portal generates a link on the camera assistance page that takes the user right to the user's router's configuration web page.

Address, Port and Where to Put Them

Since the camera's address and port are available via properties, the portal reads these properties and includes these properties in descriptive text on the camera assistance page. That page also contains a link to a router help page, where the user can select the user's router and get specific help on what to do to configure it.

Device Test

The camera assistance page has a button to test whether the port forwarding is a success or not. It uses the server's test-camera-access API to make the determination, and displays either a pass or fail message to let the user know.

Various Embodiments

In addition to the foregoing, the following are various examples of embodiments of the invention.

Some embodiments of a method for premises management networking include monitoring premises management devices connected to a gateway at a premises; controlling premises management devices connected to the gateway at the premises; receiving, at the premises, an uplink-initiation signal associated with a network operations center server; and in response to the uplink-initiation signal, initiating, from the gateway at the premises, communications between the gateway and the network operations center server; and communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices.

The uplink-initiation signal can be received via telephone and/or broadband connection. The gateway can initiate communications between the gateway and the network operations center server with at least an HTTP message and/or at least an XML message. The premises management devices can manage energy of the premises, security of the premises, and/or safety of the premises. Many embodiments provide a hosted solution for property developers, owners and managers as well as service providers (ISPs, telcos, utilities, etc.) such as communication service providers and Internet portal providers. Some embodiments offer a complete, turnkey, reliable, and/or cost-effective solution for the delivery of telemetry services (e.g., energy management, security, safety, access, health monitoring, messaging, etc.) to customers.

An embodiment of the invention is directed to a business method for premises management. Some embodiments of a business method for premises management include making an Internet portal available for access to a vendee, such as a premises vendee, communication service vendee, and/or an Internet portal vendee; and at least after a transaction between the vendor and the vendee, such as a premises transaction, a communication services transaction, and/or Internet portal services transaction, providing premises management services via the Internet portal to the vendee.

The Internet portal can be branded with a brand of the vendor according to an embodiment. Examples of a premises vendor include a home builder, premises builder, and premises manager. Examples of a premises vendee include a home buyer, premises buyer, and premises tenant. Examples of a communication service vendor include an Internet service provider, a telephone company, a satellite television company, and a cable television company. Examples of a communication service vendee include a customer of the Internet service provider, a customer of the telephone company, a customer of the satellite television company, and a customer of the cable television company. Premises management services can manage energy of the premises, security of the premises, and/or safety of the premises.

An embodiment of the invention is directed to a system. The system includes a network of premises management devices, a gateway coupled to the network and premises management devices, a server coupled to the gateway by a communication medium and a portal coupled to the communications medium. The portal provides communication with the premises management devices.

According to various embodiments in the invention alone or in various combinations: the communications medium may comprise the Internet; the portal may comprise an internet portal; and/or the portal may be branded with the name of a vendor of a product associated with the premises. The product may comprise a building, and/or the vendor may comprise a party that leases the premises. The vendor may also or alternatively comprise a property management organization. The server may be included within a network operations center. The logic may comprise, according to various embodiments of the invention, software, hardware, or a combination of software and hardware.

Another embodiment to the invention is directed to a gateway. The gateway includes an interface coupled to a network of premises management devices, logic that receives data from different premises management devices, and an interface coupled to a communications medium that is coupled to a server. The server is coupled to a portal coupled to the communications medium. The portal provides communications with the premises management devices.

According to various embodiments of the invention alone or in various combinations: the communications medium may comprise the Internet; the portal may comprise an internet to portal; and/or the portal may be branded with the name of a vendor of a product associated with the premises. The product may comprise a building; the vendor may comprise a party that leases the premises; the vendor may comprise a property management organization; and/or the server may be included within a network operations center.

Another embodiment of the invention is directed to premises management system. The premises management system includes a network of premises management devices and a gateway coupled to the network of premises management devices. The gateway includes logic that receives data from different premises management devices and an interface coupled to a communications medium that is coupled to a server. The server is coupled to a portal coupled to the communications medium, and the portal provides communication with the premises management devices. The logic may comprise, according to various embodiments of the invention, software, hardware, or a combination of software and hardware.

Another embodiment of the invention is directed to a system that includes: a network of premises management devices; a gateway coupled to the network of premises management devices; a server coupled to the gateway by a communications medium and a portal coupled to the communications medium, the portal providing communication with the premises management devices.

According to various embodiments in the invention, alone, or in various combinations: the common format includes a set of properties for each type of device; the format includes an index for each device and an index for each property of each device; the network comprises a network operations center; the network of premises management devices includes at least a camera; the system includes logic that reinterprets abstracted data in the common format from the different premises management devices; the server includes a device definition file for reinterpreting the abstracted data; the system includes a set of standard function types that define standard properties; the standard properties include temperature; the system includes client software that queries measurements corresponding to the respective property without specifying the type of device from which the measurement is to be received; the server includes a set of formatter classes that convert between the format of data in which data is passed from the gateway to the server in a type in which the data is stored in the server; the formatter classes are instantiated dynamically; the system includes device definitions for respective premises management devices; and/or the server is included within a network operations center.

An embodiment of the invention is directed to a gateway that includes: an interface coupled to a network of premises management devices; logic that abstracts data from different premises management devices using a common format; and an interface coupled to a communications medium that is coupled to a server. The server is coupled to a portal coupled to the communications medium, and the portal provides communication with the premises management devices. The gateway may include logic to interact with various aspects of the various systems described herein.

Another embodiment in the invention is directed to a gateway that includes: an interface coupled to a network of premises management devices, the network including at least a first device comprising a source of data and at least a second device comprising a recipient of the data; logic that abstracts data from different premises management devices using a common format; logic that maps data from a first device least comprising the source of data to data on a second device comprising the recipient of the data; and an interface coupled to a communications medium that is coupled to a server, wherein the server is coupled to a portal coupled to the communications medium, the portal providing communication with the premises management devices.

According to various embodiments of the invention, in various combinations or alternatively: the mapping is based on a property of the first device and a corresponding property of the second device; the mapping is stored in a table in the server; the mapping is based on a correspondence between an index of a property of the first device with an index of a property of the second device; gateway includes logic that checks whether there are any corresponding properties on a corresponding device that comprises a recipient of data if corresponding data from a device that comprises a source of the corresponding data changes; and/or the logic comprises hardware, software, or a combination of hardware and software.

Another embodiment of the invention is directed to a system that includes: a set of one or more premises management devices, the set of one or more premises management devices including at least a camera; a gateway coupled to the set of one or more network of premises management devices, the gateway including logic that abstracts data from a premises management device using a common format, general to different devices; a server coupled to the gateway by a communications medium; and a portal coupled to the communications medium, the portal providing communication with at least a device in the set of one or more premises management devices.

According to various embodiments of the invention, alternatively, or in various combinations: the system includes logic that transmits data from the gateway to the server using HTTP protocol; the data from the gateway includes an image from the camera; the gateway includes logic that pushes data to the server from the set of one or more premises management devices; the system includes logic that causes an image from the camera served from the server to be displayed; the system includes logic that causes an image from the camera to be transmitted from the gateway to the server in response to an uplink-initiation signal; the uplink communication signal is received via telephone; the uplink communication signal is received via telephone without requiring answering of a telephone call; the uplink communication signal is received via broadband connection; at least a device in the set of one or more network of premises management devices manages energy of the premises; at least a device in the set of one or more network of premises management devices manages security of the premises; at least a device in the set of one or more network of premises management devices manages safety of the premises; the camera includes at least a property specific to a camera and at least a property common with at least another type of device; the property specific to a camera causes the camera to take a picture; the property specific to a camera causes a picture taken by the camera to be uploaded to the server; the system includes logic that causes a picture to be taken based on the state of another device in the set of one or more premises management devices; another device in the set comprises a motion sensor; the system includes the plurality of different types of cameras and wherein the gateway includes logic that abstracts data from the different types of cameras into a common format for delivery to the server; the system includes a router that couples the gateway to the communications medium; the camera comprises an internet protocol (IP) camera; and images from the camera are provided over the communications medium only if the gateway initiates a transfer of the image to the server.

Another embodiment of the invention is directed to a system that includes: a set of one or more premises management devices, the set of one or more premises management devices including at least a camera; a gateway coupled to the set of one or more network of premises management devices; a server coupled to the gateway by a communications medium, and a portal coupled to the communications medium, the portal providing communication with at least a device in the set of one or more premises management devices. The gateway includes logic that pushes data from the set of one or more premises management devices to the server.

According to various embodiments of the invention, alternatively, or in various combinations: the gateway does not allow direct access to the set of one or more premises. management devices from the communications medium; the system includes logic that causes an image from the camera to be transmitted from the gateway to the server in response to an uplink-initiation signal; the uplink communication signal is received via telephone; the uplink communication signal is received via telephone without requiring answering of a telephone call; the uplink communication signal is received via broadband connection; at least a device in the set of one or more network of premises management devices manages security of the premises; the camera includes at least a property specific to a camera and at least a property common with at least another type of device; the property specific to a camera causes the camera to take a picture; the system includes logic that causes a picture to be taken based on the state of another device in the set of one or more premises management devices; the system includes a plurality of different types of cameras and the gateway includes logic that abstracts data from the different types of cameras into a common format for delivery to the server; and/or the camera comprises an internet protocol (IP) camera.

Another embodiment of the invention is directed to a gateway that includes: an interface coupled to a set of one or more premises management devices, the set of one or more premises management devices including at least a camera; and an interface coupled to a communications medium that is coupled to a server, wherein the server is coupled to a portal coupled to the communications medium, the portal providing communication with the premises management devices; and logic that pushes data from one or more premises management devices to the server.

Components of the gateway, server, system and/or other aspects described above include any collection of computing components and devices operating together. Components of these items can also be components of subsystems or within a larger computer system or network. The components can also be coupled among any number of components (not shown), for example other buses, controllers, memory devices and data input/output (IO) devices in any number of combinations. Further common components of these items can be distributed among various numbers or combinations of other processor-based components according to various embodiments of the invention.

Aspects of the gateway, server, system and other items described here and may be implemented as functionality programmed into any variety of circuitry, including programmable logic devices, (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects these items include: microcontrollers with memory (such as electronically erasable programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the gateway, server and other elements may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

The various functions or processes disclosed herein may be described as data and/or instructions embodied in various non-transitory computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., HTTP, FTP, SMTP, etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of components and/or processes under the ICS may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

Unless the context clearly requires otherwise, throughout the description and the claims, the words “comprise,” “comprising,” and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of “including, but not limited to.” Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words “herein,” “hereunder,” “above,” “below,” and words of similar import refer to this application as a whole and not to any particular portions of this application. When the word “or” is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

The above description of illustrated embodiments of the system is not intended to be exhaustive or to limit the system to the precise form disclosed. While specific embodiments of, and examples for, the system are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the system, as those skilled in the relevant art will recognize. The teachings of the system provided herein can be applied to other processing systems and methods, not only for the systems and methods described above.

The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the system in light of the above detailed description.

In general, in the following claims, the terms used should not be construed to limit the system to the specific embodiments disclosed in the specification and the claims, but should be construed to include all processing systems that operate under the claims. Accordingly, the system is not limited by the disclosure, but instead the scope of the system is to be determined entirely by the claims.

While certain aspects of the system are presented below in certain claim forms, the inventors contemplate the various aspects of the system in any number of claim forms. For example, while only one aspect of the system is recited as embodied in machine-readable medium, other aspects may likewise be embodied in machine-readable medium. Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the system.

What is claimed is:

1. A method for premises management networking of a premises management system, the method comprising:

monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices form a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks;

controlling the premises management devices, the controlling comprising the gateway selectively forming and controlling an associative binding between the plurality of networks;

obtaining an assigned server address, and using the assigned server address for all subsequent uplink connections unless the assigned server address is changed later by the system;

initiating, by the gateway, all communications with a network operations center server using the assigned server address; and

communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices, wherein the assigned server address is an address associated with the network operations center server.

2. The method of claim **1**, wherein the uplink-initiation signal is received via telephone.

3. The method of claim **1**, wherein the uplink-initiation signal is received via broadband connection.

4. The method of claim **1**, wherein the gateway initiates communications between the gateway and the network operations center server with at least an HTTP message.

5. The method of claim **1**, wherein the gateway initiates communications between the gateway and the network operations center server with at least an XML message.

6. The method of claim **1**, wherein the premises management devices manage energy of the premises.

7. The method of claim **1**, wherein the premises management devices manage security of the premises.

8. The method of claim **1**, wherein the premises management devices manage safety of the premises.

9. The method of claim **1**, wherein the plurality of networks includes a security network and an Internet Protocol (IP) device network.

10. The method of claim **1**, wherein the plurality of networks includes a security network and an energy control network.

11. The method of claim **1**, wherein the plurality of networks includes an Internet Protocol (IP) device network and an energy control network.

12. The method of claim **1**, wherein the plurality of networks includes a security network, an Internet Protocol (IP) network, and an energy control network.

13. The method of claim **1**, wherein the plurality of networks includes a legacy security system, wherein the gateway is connected to a controller of the legacy security system.

14. A premises management networking gateway of a premises management system, the gateway including a computer readable medium having data, instructions or a combination thereof for managing a premises network, comprising:

non-transitory computer readable medium having data, instructions or a combination thereof for monitoring premises management devices connected to the gateway at a premises, wherein the premises management devices form a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks;

non-transitory computer readable medium having data, instructions or a combination thereof for controlling the premises management devices, the controlling comprising the gateway selectively forming and controlling an associative binding between the plurality of networks;

non-transitory computer readable medium having data, instructions or a combination thereof for obtaining an assigned server address, and using the assigned server address for all subsequent uplink connections unless the assigned server address is changed later by the system;

non-transitory computer readable medium having data, instructions or a combination thereof for initiating, by the gateway, all communications with a network operations center server using the assigned server address; and

non-transitory computer readable medium having data, instructions or a combination thereof for communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices, wherein the assigned server address is an address associated with the network operations center server.

15. The premises management networking gateway of claim **14**, wherein the uplink-initiation signal is received via telephone.

16. The premises management networking gateway of claim **14**, wherein the uplink-initiation signal is received via broadband connection.

17. The premises management networking gateway of claim **14**, wherein the gateway initiates communications between the gateway and the network operations center server with at least an HTTP message.

18. The premises management networking gateway of claim **14**, wherein the gateway initiates communications between the gateway and the network operations center server with at least an XML message.

19. The premises management networking gateway of claim 14, wherein the premises management devices manage energy of the premises.

20. The premises management networking gateway of claim 14, wherein the premises management devices manage security of the premises.

21. The premises management networking gateway of claim 14, wherein the premises management devices manage safety of the premises.

22. The premises management networking gateway of claim 14, wherein the plurality of networks includes a security network and an Internet Protocol (IP) device network.

23. The premises management networking gateway of claim 9, wherein the plurality of networks includes a security network and an energy control network.

24. The premises management networking gateway of claim 14, wherein the plurality of networks includes an Internet Protocol (IP) device network and an energy control network.

25. The premises management networking gateway of claim 14, wherein the plurality of networks includes a security network, an Internet Protocol (IP) network, and an energy control network.

* * * * *

EXHIBIT 4

US008612591B2

(12) **United States Patent**
Dawes et al.

(10) **Patent No.: US 8,612,591 B2**
(45) **Date of Patent: *Dec. 17, 2013**

(54) **SECURITY SYSTEM WITH NETWORKED TOUCHSCREEN**

(75) Inventors: **Paul J. Dawes**, Woodside, CA (US); **Jim Fulker**, Palo Alto, CA (US); **Carolyn Wales**, Menlo Park, CA (US)

(73) Assignee: **iControl Networks, Inc.**, Redwood City, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 462 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/197,946**

(22) Filed: **Aug. 25, 2008**

(65) **Prior Publication Data**

US 2009/0070682 A1 Mar. 12, 2009

Related U.S. Application Data

(63) Continuation-in-part of application No. 11/084,232, filed on Mar. 16, 2005, and a continuation-in-part of application No. 11/761,718, filed on Jun. 12, 2007, now Pat. No. 7,711,796, and a continuation-in-part of application No. 11/761,745, filed on Jun. 12, 2007, and a continuation-in-part of application No. 12/019,554, filed on Jan. 24, 2008, and a continuation-in-part of application No. 12/019,568, filed on Jan. 24, 2008, and

(Continued)

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.**
USPC **709/225**; 709/219

(58) **Field of Classification Search**
USPC 709/225
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,754,261 A 6/1988 Marino
4,779,007 A 10/1988 Schlanger et al.

(Continued)

FOREIGN PATENT DOCUMENTS

JP 2003/085258 A 9/2001
JP 2003/141659 10/2001

(Continued)

OTHER PUBLICATIONS

Form PCT/ISA/220, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.

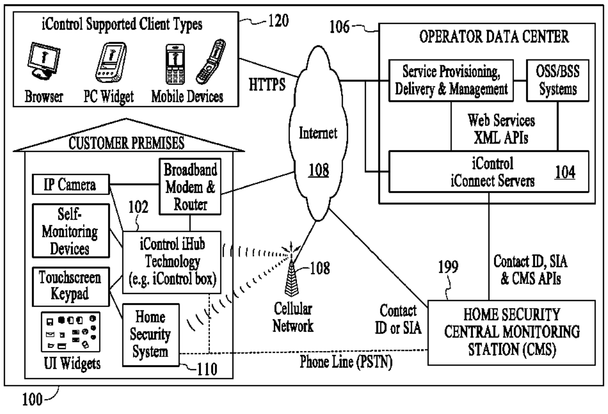
(Continued)

Primary Examiner — Tauqir Hussain
(74) *Attorney, Agent, or Firm* — Gregory & Sawrie LLP

(57) **ABSTRACT**

An integrated security system integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network that with remote connectivity and access. The integrated security system includes a touchscreen providing security keypad functionality as well as content management and presentation, and is used as a security system interface and an interface for interacting with a network. The integrated security system delivers remote premise monitoring and control functionality to conventional monitored premise protection and complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices can be added, enabling users to remotely see live video or pictures and control home devices via a personal web portal, mobile phone, or other client device. Users can receive notifications of detected events via electronic message.

58 Claims, 18 Drawing Sheets


iControl Supported Client Types
Browser
PC Widget
Mobile Devices
120
106
HTTPS
OPERATOR DATA CENTER
Service Provisioning, Delivery & Management
OSS/BSS Systems
Web Services XML APIs
Internet
108
iControl iConnect Servers
104
CUSTOMER PREMISES
IP Camera
Broadband Modem & Router
102
Self-Monitoring Devices
iControl iHub Technology (e.g. iControl box)
108
Touchscreen Keypad
199
Contact ID, SIA & CMS APIs
Home Security System
Cellular Network
Contact ID or SIA
HOME SECURITY CENTRAL MONITORING STATION (CMS)
UI Widgets
110
Phone Line (PSTN)
100

Related U.S. Application Data

(63) a continuation-in-part of application No. 12/189,757, filed on Aug. 11, 2008.

(60) Provisional application No. 60/957,997, filed on Aug. 24, 2007, provisional application No. 60/968,005, filed on Aug. 24, 2007, provisional application No. 60/987,359, filed on Nov. 12, 2007, provisional application No. 60/987,366, filed on Nov. 12, 2007, provisional application No. 61/019,162, filed on Jan. 4, 2008, provisional application No. 61/019,167, filed on Jan. 4, 2008, provisional application No. 61/023,489, filed on Jan. 25, 2008, provisional application No. 61/023,493, filed on Jan. 25, 2008, provisional application No. 61/023,496, filed on Jan. 25, 2008, provisional application No. 61/087,967, filed on Aug. 11, 2008.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,833,449 A 5/1989 Gaffigan
4,860,185 A 8/1989 Brewer et al.
4,993,059 A 2/1991 Smith et al.
5,086,385 A 2/1992 Launey et al.
5,519,878 A 5/1996 Dolin, Jr.
5,579,197 A 11/1996 Mengelt et al.
5,907,279 A 5/1999 Bruins et al.
5,963,916 A 10/1999 Kaplan
D416,910 S 11/1999 Vasquez
5,991,795 A 11/1999 Howard et al.
6,037,991 A 3/2000 Thro et al.
6,052,052 A 4/2000 Delmonaco
6,060,994 A 5/2000 Chen
6,134,591 A 10/2000 Nickles
6,140,987 A 10/2000 Stein et al.
6,198,479 B1 3/2001 Humpleman et al.
6,219,677 B1 4/2001 Howard
6,281,790 B1 8/2001 Kimmel et al.
6,286,038 B1 9/2001 Reichmeyer et al.
6,288,716 B1 9/2001 Humpleman et al.
D451,529 S 12/2001 Vasquez
6,331,122 B1 12/2001 Wu
6,351,829 B1 2/2002 Dupont et al.
6,353,891 B1 3/2002 Borella et al.
6,363,417 B1 3/2002 Howard et al.
6,370,436 B1 4/2002 Howard et al.
6,377,861 B1 4/2002 York
6,385,772 B1 5/2002 Courtney
6,400,265 B1 6/2002 Saylor et al.
D464,328 S 10/2002 Vasquez et al.
D464,948 S 10/2002 Vasquez et al.
6,462,507 B2 10/2002 Fisher, Jr.
6,462,663 B1 10/2002 Wilson et al.
6,467,084 B1 10/2002 Howard et al.
6,480,901 B1 11/2002 Weber et al.
6,493,020 B1 12/2002 Stevenson et al.
6,496,927 B1 12/2002 McGrane
6,529,723 B1 3/2003 Bentley
6,542,075 B2 4/2003 Barker et al.
6,563,800 B1 5/2003 Salo et al.
6,574,234 B1 6/2003 Myer et al.
6,580,950 B1 6/2003 Johnson et al.
6,587,736 B2 7/2003 Howard et al.
6,591,094 B1 7/2003 Bentley
6,601,086 B1 7/2003 Howard et al.
6,609,127 B1 8/2003 Lee et al.
6,615,088 B1 9/2003 Myer et al.
6,621,827 B1 9/2003 Rezvani et al.
6,643,652 B2 11/2003 Helgeson et al.
6,643,669 B1 11/2003 Novak et al.
6,648,682 B1 11/2003 Wu
6,658,091 B1 12/2003 Naidoo et al.
6,661,340 B1 12/2003 Saylor et al.
6,686,838 B1 2/2004 Rezvani et al.
6,690,411 B2 2/2004 Naidoo et al.
6,693,545 B2 2/2004 Brown et al.
6,721,689 B2 4/2004 Markle et al.
6,721,747 B2 4/2004 Lipkin
6,738,824 B1 5/2004 Blair
6,756,998 B1 6/2004 Bilger
6,778,085 B2 8/2004 Faulkner et al.
6,781,509 B1 8/2004 Oppedahl et al.
6,789,147 B1 9/2004 Kessler et al.
6,795,322 B2 9/2004 Aihara et al.
6,798,344 B2 9/2004 Faulkner et al.
6,826,233 B1 11/2004 Oosawa
6,865,690 B2 3/2005 Kocin
6,891,838 B1 5/2005 Petite et al.
6,912,429 B1 6/2005 Bilger
6,928,148 B2 8/2005 Simon et al.
6,930,599 B2 8/2005 Naidoo et al.
6,930,730 B2 8/2005 Maxon et al.
6,931,445 B2 8/2005 Davis
6,943,681 B2 9/2005 Rezvani et al.
6,959,393 B2 10/2005 Hollis et al.
6,965,313 B1 11/2005 Saylor et al.
6,970,183 B1 11/2005 Monroe
6,972,676 B1 12/2005 Kimmel et al.
6,975,220 B1 12/2005 Foodman et al.
6,990,591 B1 1/2006 Pearson
7,016,970 B2 3/2006 Harumoto et al.
7,024,676 B1 4/2006 Klopfenstein
7,030,752 B2 4/2006 Tyroler
7,032,002 B1 4/2006 Rezvani et al.
7,034,681 B2 4/2006 Yamamoto et al.
7,039,391 B2 5/2006 Rezvani et al.
7,047,088 B2 5/2006 Nakamura et al.
7,047,092 B2 5/2006 Wimsatt
7,072,934 B2 7/2006 Helgeson et al.
7,079,020 B2 7/2006 Stilp
7,080,046 B1 7/2006 Rezvani et al.
7,085,937 B1 8/2006 Rezvani et al.
7,099,994 B2 8/2006 Thayer et al.
7,103,152 B2 9/2006 Naidoo et al.
7,106,176 B2 9/2006 La et al.
7,113,090 B1 * 9/2006 Saylor et al. 340/539.18
7,113,099 B2 9/2006 Tyroler et al.
7,120,232 B2 10/2006 Naidoo et al.
7,120,233 B2 10/2006 Naidoo et al.
7,130,383 B2 10/2006 Naidoo et al.
7,130,585 B1 10/2006 Ollis et al.
7,148,810 B2 12/2006 Bhat
7,149,798 B2 12/2006 Rezvani et al.
7,174,564 B1 2/2007 Weatherspoon et al.
7,183,907 B2 2/2007 Simon et al.
7,203,486 B2 4/2007 Patel
7,218,217 B2 5/2007 Adonailo et al.
7,222,359 B2 5/2007 Freund et al.
7,237,267 B2 6/2007 Rayes et al.
7,250,854 B2 7/2007 Rezvani et al.
7,254,779 B1 8/2007 Rezvani et al.
7,262,690 B2 8/2007 Heaton et al.
7,305,461 B2 12/2007 Ullmann
7,337,217 B2 2/2008 Wang
7,337,473 B2 2/2008 Chang et al.
7,343,619 B2 3/2008 Ofek et al.
7,349,761 B1 3/2008 Cruse
7,349,967 B2 3/2008 Wang
7,367,045 B2 4/2008 Ofek et al.
7,370,115 B2 5/2008 Bae et al.
7,383,339 B1 6/2008 Meenan et al.
7,403,838 B2 7/2008 Deen et al.
7,409,451 B1 8/2008 Meenan et al.
7,428,585 B1 9/2008 Owens et al.
7,430,614 B2 9/2008 Shen et al.
7,440,434 B2 10/2008 Chaskar et al.
7,457,869 B2 11/2008 Kernan
7,469,139 B2 12/2008 van de Groenendaal
7,469,294 B1 12/2008 Luo et al.
7,480,713 B2 1/2009 Ullman
7,480,724 B2 1/2009 Zimler et al.
7,506,052 B2 3/2009 Qian et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,509,687	B2	3/2009	Ofek et al.	
7,526,762	B1	4/2009	Astala et al.	
7,551,071	B2	6/2009	Bennett, III et al.	
7,558,379	B2	7/2009	Winick	
7,577,420	B2	8/2009	Srinivasan et al.	
7,587,464	B2	9/2009	Moorer et al.	
7,627,665	B2	12/2009	Barker et al.	
7,634,519	B2	12/2009	Creamer et al.	
2001/0016501	A1	8/2001	King	
2001/0034754	A1	10/2001	Elwahab et al.	
2002/0004828	A1	1/2002	Davis et al.	
2002/0026476	A1	2/2002	Miyazaki et al.	
2002/0029276	A1	3/2002	Bendinelli et al.	
2002/0038380	A1	3/2002	Brawn et al.	
2002/0052913	A1	5/2002	Yamada et al.	
2002/0083342	A1	6/2002	Webb et al.	
2002/0095490	A1	7/2002	Barker et al.	
2002/0103898	A1	8/2002	Moyer et al.	
2002/0103927	A1	8/2002	Parent	
2002/0107910	A1	8/2002	Zhao	
2002/0111698	A1	8/2002	Graziano et al.	
2002/0112051	A1	8/2002	Ullmann	
2002/0112182	A1	8/2002	Chang et al.	
2002/0143923	A1	10/2002	Alexander	
2002/0156564	A1	10/2002	Preston et al.	
2002/0180579	A1	12/2002	Nagoka et al.	
2002/0184301	A1	12/2002	Parent	
2003/0009552	A1	1/2003	Benfield et al.	
2003/0009553	A1	1/2003	Benfield et al.	
2003/0041167	A1	2/2003	French et al.	
2003/0051009	A1	3/2003	Shah et al.	
2003/0052923	A1	3/2003	Porter	
2003/0062997	A1	4/2003	Naidoo et al.	
2003/0090473	A1	5/2003	Joshi	
2003/0115345	A1	6/2003	Chien et al.	
2003/0132018	A1	7/2003	Okita et al.	
2003/0174648	A1	9/2003	Wang et al.	
2003/0187920	A1	10/2003	Redkar	
2003/0210126	A1	11/2003	Kanazawa	
2003/0236841	A1	12/2003	Epshteyn	
2004/0003241	A1	1/2004	Sengodan et al.	
2004/0015572	A1	1/2004	Kang	
2004/0037295	A1	2/2004	Tanaka et al.	
2004/0054789	A1	3/2004	Breh et al.	
2004/0086088	A1	5/2004	Naidoo et al.	
2004/0123149	A1	6/2004	Tyroler	
2004/0139227	A1	7/2004	Takeda	
2004/0162902	A1	8/2004	Davis	
2004/0177163	A1	9/2004	Casey et al.	
2004/0243835	A1	12/2004	Terzis et al.	
2004/0267937	A1	12/2004	Klements	
2005/0038326	A1	2/2005	Mathur	
2005/0066045	A1	3/2005	Johnson et al.	
2005/0069098	A1	3/2005	Kalervo et al.	
2005/0079855	A1	4/2005	Jethi et al.	
2005/0086126	A1	4/2005	Patterson	
2005/0108091	A1	5/2005	Sotak et al.	
2005/0108369	A1	5/2005	Sather et al.	
2005/0125083	A1	6/2005	Kiko	
2005/0128083	A1 *	6/2005	Puzio et al.	340/572.1
2005/0149639	A1	7/2005	Vrielink et al.	
2005/0169288	A1	8/2005	Kamiwada et al.	
2005/0197847	A1	9/2005	Smith	
2005/0216302	A1	9/2005	Raji et al.	
2005/0216580	A1	9/2005	Raji et al.	
2005/0222820	A1	10/2005	Chung	
2005/0231349	A1	10/2005	Bhat	
2006/0009863	A1	1/2006	Lingemann	
2006/0088092	A1	4/2006	Chen et al.	
2006/0105713	A1	5/2006	Zheng et al.	
2006/0111095	A1	5/2006	Weigand	
2006/0181406	A1	8/2006	Petite et al.	
2006/0182100	A1	8/2006	Li et al.	
2006/0187900	A1	8/2006	Akbar	
2006/0200845	A1	9/2006	Foster et al.	
2006/0206220	A1	9/2006	Amundson	
2006/0271695	A1	11/2006	Lavian	
2006/0282886	A1	12/2006	Gaug	
2007/0052675	A1	3/2007	Chang	
2007/0061266	A1	3/2007	Moore et al.	
2007/0106124	A1	5/2007	Kuriyama et al.	
2007/0142022	A1 *	6/2007	Madonna et al.	455/352
2007/0256105	A1	11/2007	Tabe	
2007/0286210	A1	12/2007	Gutt et al.	
2007/0286369	A1	12/2007	Gutt et al.	
2007/0298772	A1	12/2007	Owens et al.	
2008/0042826	A1	2/2008	Hevia et al.	
2008/0065681	A1	3/2008	Fontijn et al.	
2008/0084296	A1	4/2008	Kutzik et al.	
2008/0147834	A1	6/2008	Quinn et al.	
2008/0180240	A1	7/2008	Raji et al.	
2008/0183842	A1	7/2008	Raji et al.	
2008/0235326	A1	9/2008	Parsi et al.	
2009/0070436	A1	3/2009	Dawes et al.	
2009/0070681	A1 *	3/2009	Dawes et al.	715/736
2009/0070682	A1 *	3/2009	Dawes et al.	715/736
2009/0070692	A1 *	3/2009	Dawes et al.	715/764
2009/0077622	A1 *	3/2009	Baum et al.	726/1
2009/0165114	A1	6/2009	Baum et al.	
2009/0204693	A1	8/2009	Andreev et al.	
2009/0240787	A1	9/2009	Denny	
2009/0240814	A1	9/2009	Brubacher et al.	
2010/0082744	A1	4/2010	Gutt	
2010/0095111	A1	4/2010	Gutt	
2010/0095369	A1	4/2010	Gutt	

FOREIGN PATENT DOCUMENTS

JP	2004/192659		2/2004
KR	2006/0021605		9/2004
WO	WO 89/07855		8/1989
WO	WO 01/52478		7/2001
WO	WO 01/99078		12/2001
WO	WO 2004/004222		1/2004
WO	WO 2004/107710		12/2004
WO	WO 2005/091218	A2	9/2005
WO	WO 2005/091218	A3	9/2005

OTHER PUBLICATIONS

Form PCT/ISA/210, "PCT International Search Report," 2 pgs.

Form PCT/ISA/237, "PCT Written Opinion of the International Searching Authority," 8 pgs.

Form PCT/ISA/237, "PCT Written Opinion of the International Searching Authority," 6 pgs.

Form PCT/ISA/237, "PCT Written Opinion of the International Searching Authority," 7 pgs.

Form PCT/ISA/237, PCT/US05/08766, "PCT Written Opinion of the International Searching Authority," 5 pgs.

Examination Report under Section 18(3) re UK patent application No. GB0724760.4 dated Jan. 30, 2008 4 pgs.

Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jan. 30, 2008 4 pgs.

Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jun. 4, 2008 2 pgs.

Examination Report under Section 18(3) re UK patent application No. GB0800040.8 dated Jan. 30, 2008 4 pgs.

Examination Report under Section 18(3) re UK patent application No. GB0620362.4 dated Aug. 13, 2007, 3 pgs.

Alarm.com—Interactive Security Systems, Product Advantages, printed from website Nov. 4, 2003, 3 pp.

Alarm.com—Interactive Security Systems, Frequently Asked Questions, printed from website Nov. 4, 2003, 3 pp.

Alarm.com—Interactive Security Systems, Elders, printed from website Nov. 4, 2003, 1 page.

Alarm.com—Interactive Security Systems, Overview, printed from website Nov. 4, 2003, 2 pp.

X10—ActiveHome, Home Automation Made Easy!, printed from website Nov. 4, 2003, 3 pp.

* cited by examiner

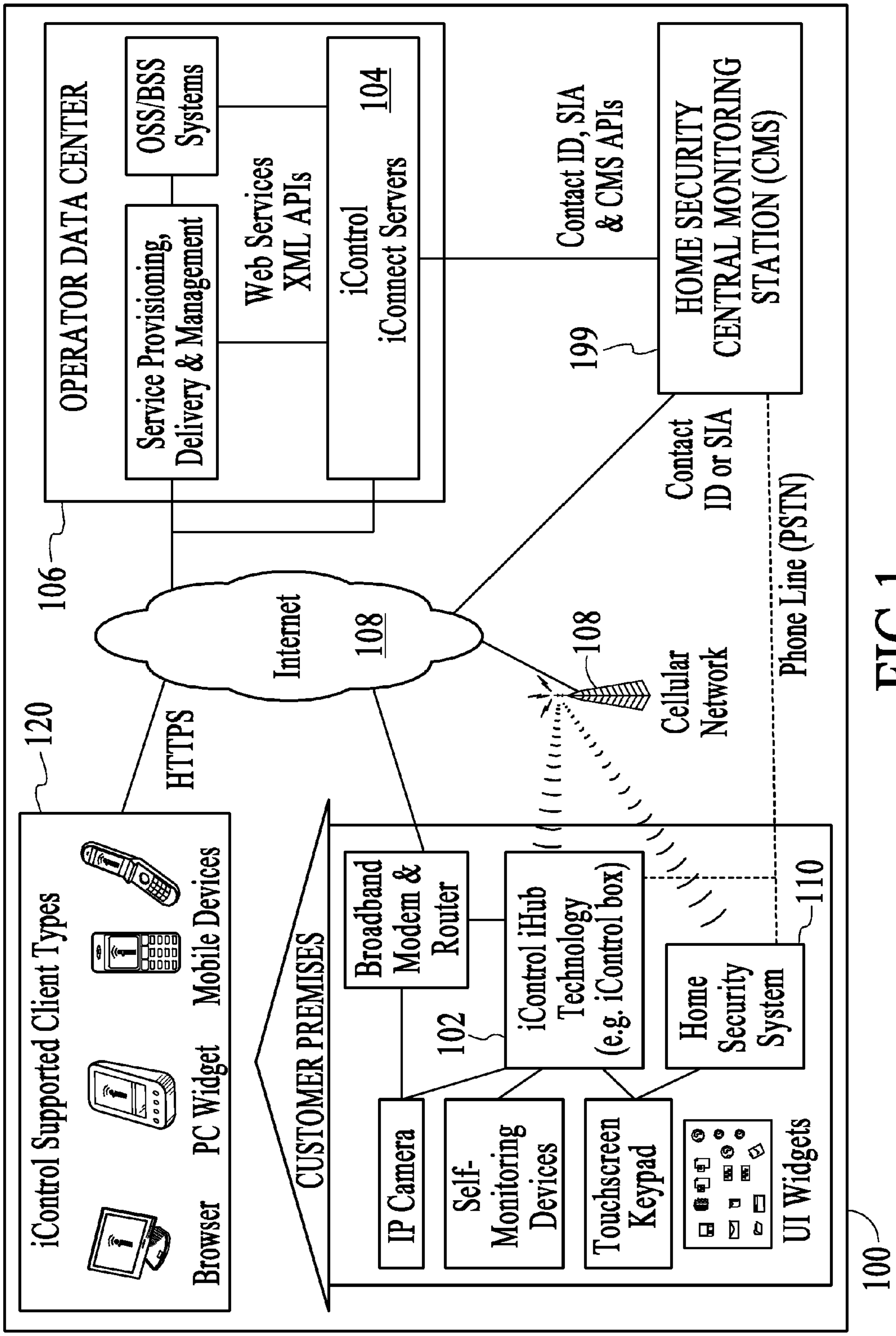

OPERATOR DATA CENTER
Service Provisioning, Delivery & Management
OSS/BSS Systems
Web Services XML APIs
iControl iConnect Servers
104
106
Contact ID, SIA & CMS APIs
HOME SECURITY CENTRAL MONITORING STATION (CMS)
199
Contact ID or SIA
Phone Line (PSTN)
Internet
108
Cellular Network
108
120
iControl Supported Client Types
Browser
PC Widget
Mobile Devices
HTTPS
CUSTOMER PREMISES
Broadband Modem & Router
iControl iHub Technology (e.g. iControl box)
102
Home Security System
110
IP Camera
Self-Monitoring Devices
Touchscreen Keypad
UI Widgets
100

FIG.1

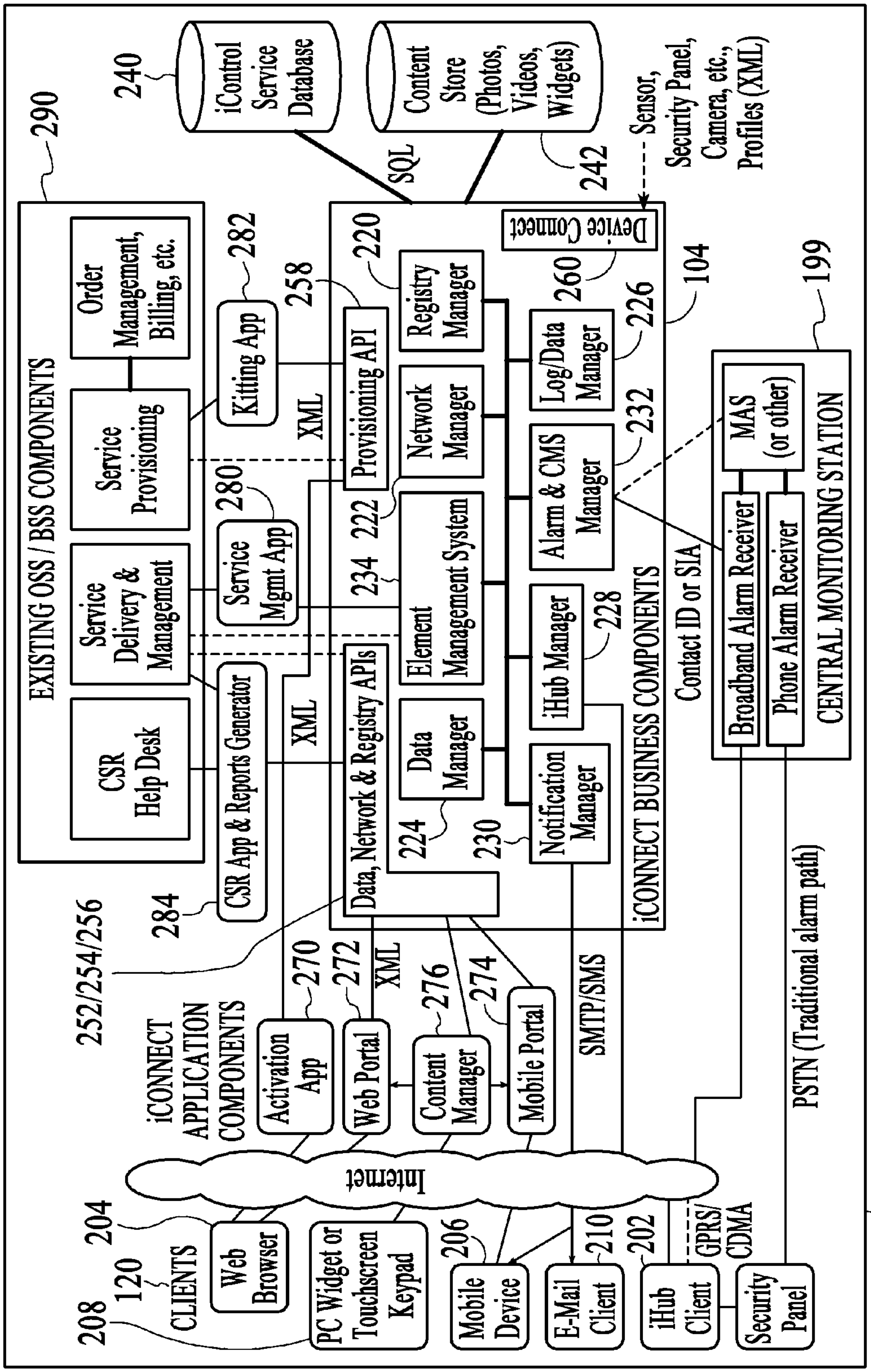

100
290
EXISTING OSS / BSS COMPONENTS
CSR Help Desk
Service Delivery & Management
Service Provisioning
Order Management, Billing, etc.
284
CSR App & Reports Generator
Service Mgmt App
280
Kitting App
282
XML
258
220
Provisioning API
Data, Network & Registry APIs
252/254/256
224
Data Manager
234
222
Element Management System
Network Manager
Registry Manager
230
Notification Manager
iHub Manager
228
Alarm & CMS Manager
232
Log/Data Manager
226
260
Device Connect
104
iCONNECT BUSINESS COMPONENTS
Contact ID or SIA
SQL
240
iControl Service Database
Content Store (Photos, Videos, Widgets)
242
Sensor, Security Panel, Camera, etc., Profiles (XML)
199
Broadband Alarm Receiver
Phone Alarm Receiver
MAS (or other)
CENTRAL MONITORING STATION
iCONNECT APPLICATION COMPONENTS
Activation App
270
Web Portal
272
Content Manager
276
Mobile Portal
274
SMTP/SMS
PSTN (Traditional alarm path)
Internet
208
120
CLIENTS
204
Web Browser
PC Widget or Touchscreen Keypad
206
Mobile Device
210
E-Mail Client
202
iHub Client
GPRS/ CDMA
Security Panel

FIG.2

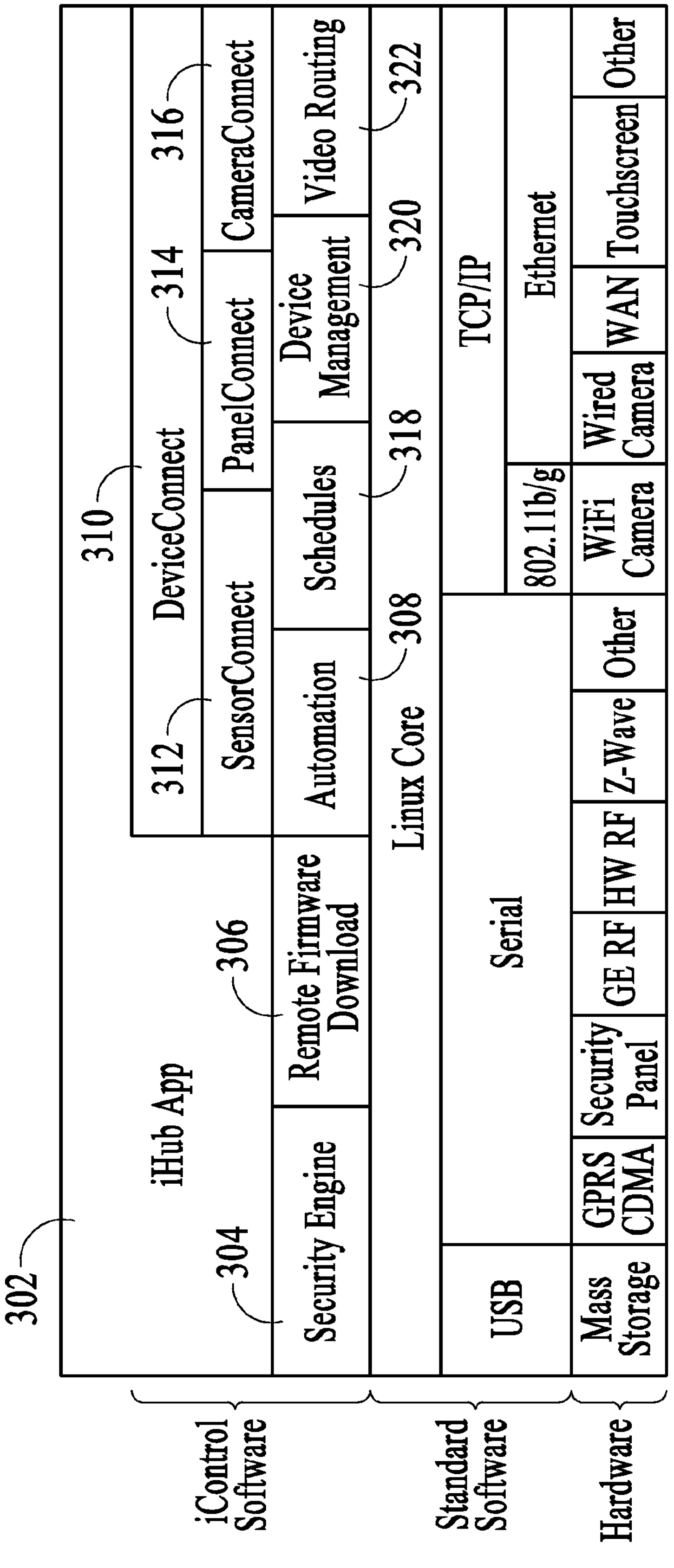

102
302
iHub App
304
Security Engine
306
Remote Firmware Download
310
DeviceConnect
312
SensorConnect
314
PanelConnect
316
CameraConnect
308
Automation
318
Schedules
320
Device Management
322
Video Routing
Linux Core
USB
Serial
TCP/IP
802.11b/g
Ethernet
Mass Storage
GPRS CDMA
Security Panel
GE RF
HW RF
Z-Wave
Other
WiFi Camera
Wired Camera
WAN
Touchscreen
Other
iControl Software
Standard Software
Hardware

FIG. 3

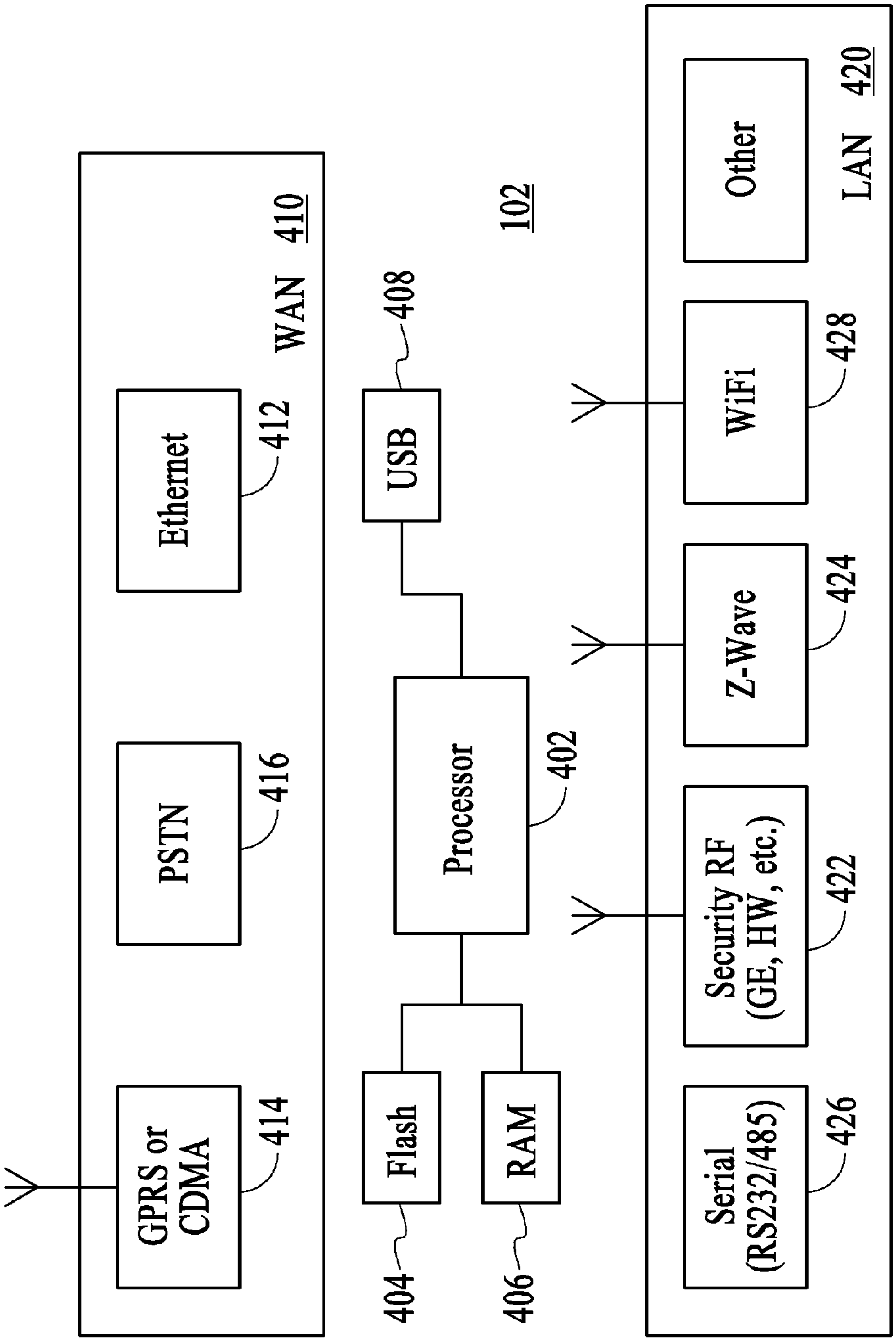

102
WAN 410
Ethernet
412
PSTN
416
GPRS or CDMA
414
USB
408
Processor
402
Flash
404
RAM
406
LAN 420
Other
WiFi
428
Z-Wave
424
Security RF (GE, HW, etc.)
422
Serial (RS232/485)
426

FIG.4

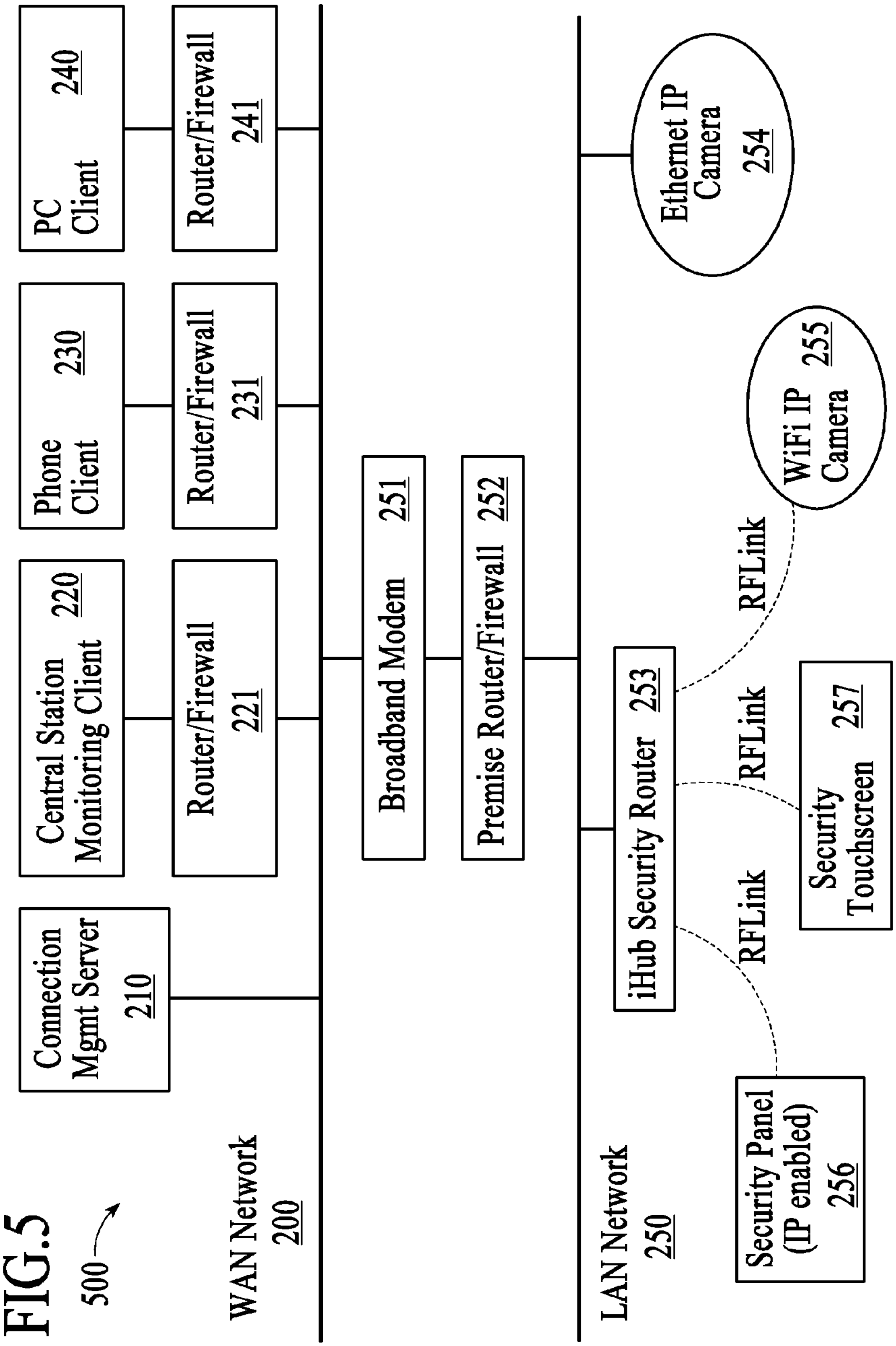
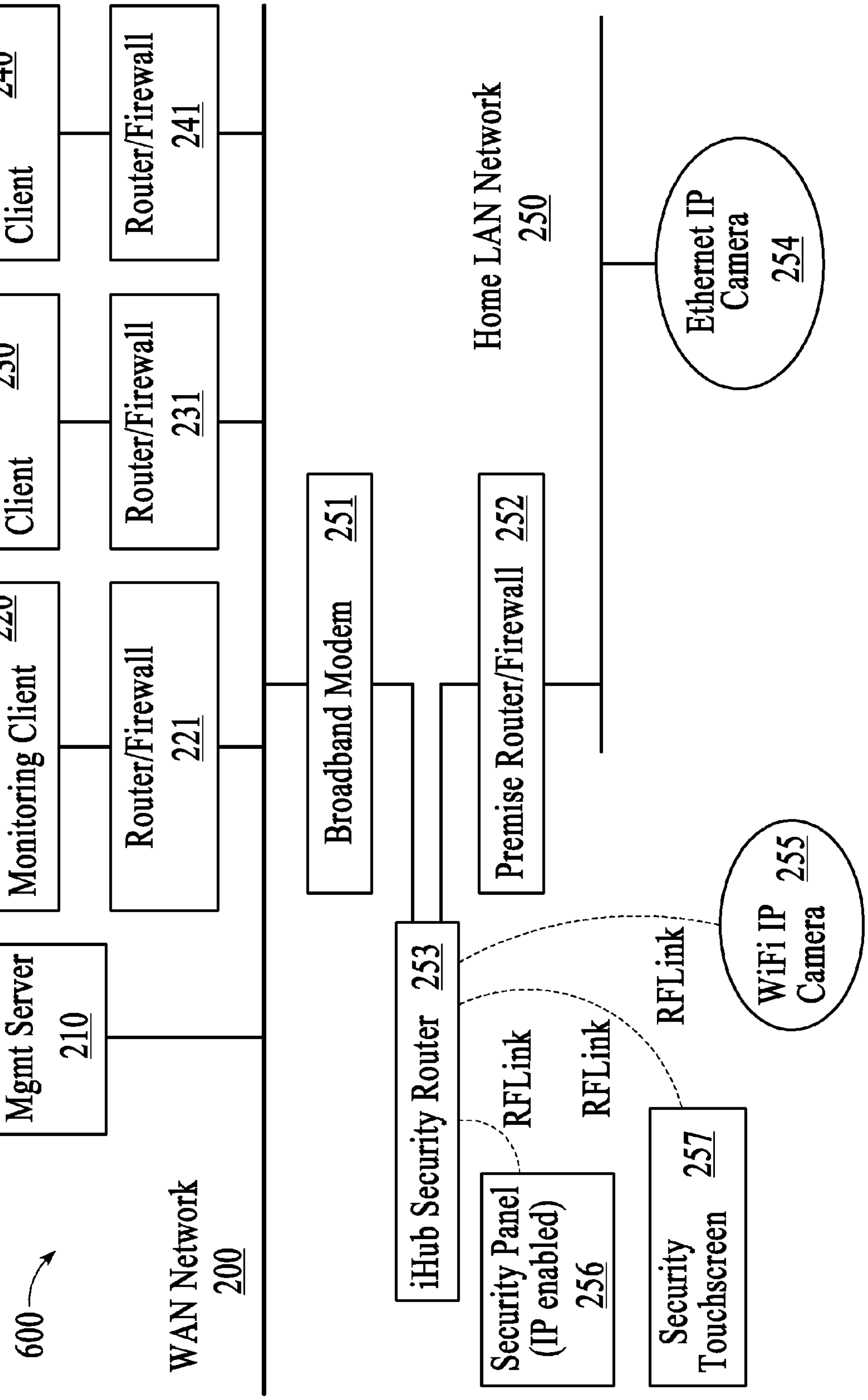

500
WAN Network 200
Connection Mgmt Server 210
Central Station Monitoring Client 220
Router/Firewall 221
Phone Client 230
Router/Firewall 231
PC Client 240
Router/Firewall 241
Broadband Modem 251
Premise Router/Firewall 252
LAN Network 250
iHub Security Router 253
Ethernet IP Camera 254
WiFi IP Camera 255
Security Panel (IP enabled) 256
Security Touchscreen 257
RFLink
RFLink
RFLink

FIG.5

FIG.6


600
WAN Network 200
Connection Mgmt Server 210
Central Station Monitoring Client 220
Router/Firewall 221
Phone Client 230
Router/Firewall 231
PC Client 240
Router/Firewall 241
Broadband Modem 251
Premise Router/Firewall 252
Home LAN Network 250
Ethernet IP Camera 254
iHub Security Router 253
WiFi IP Camera 255
RFLink
RFLink
RFLink
Security Panel (IP enabled) 256
Security Touchscreen 257

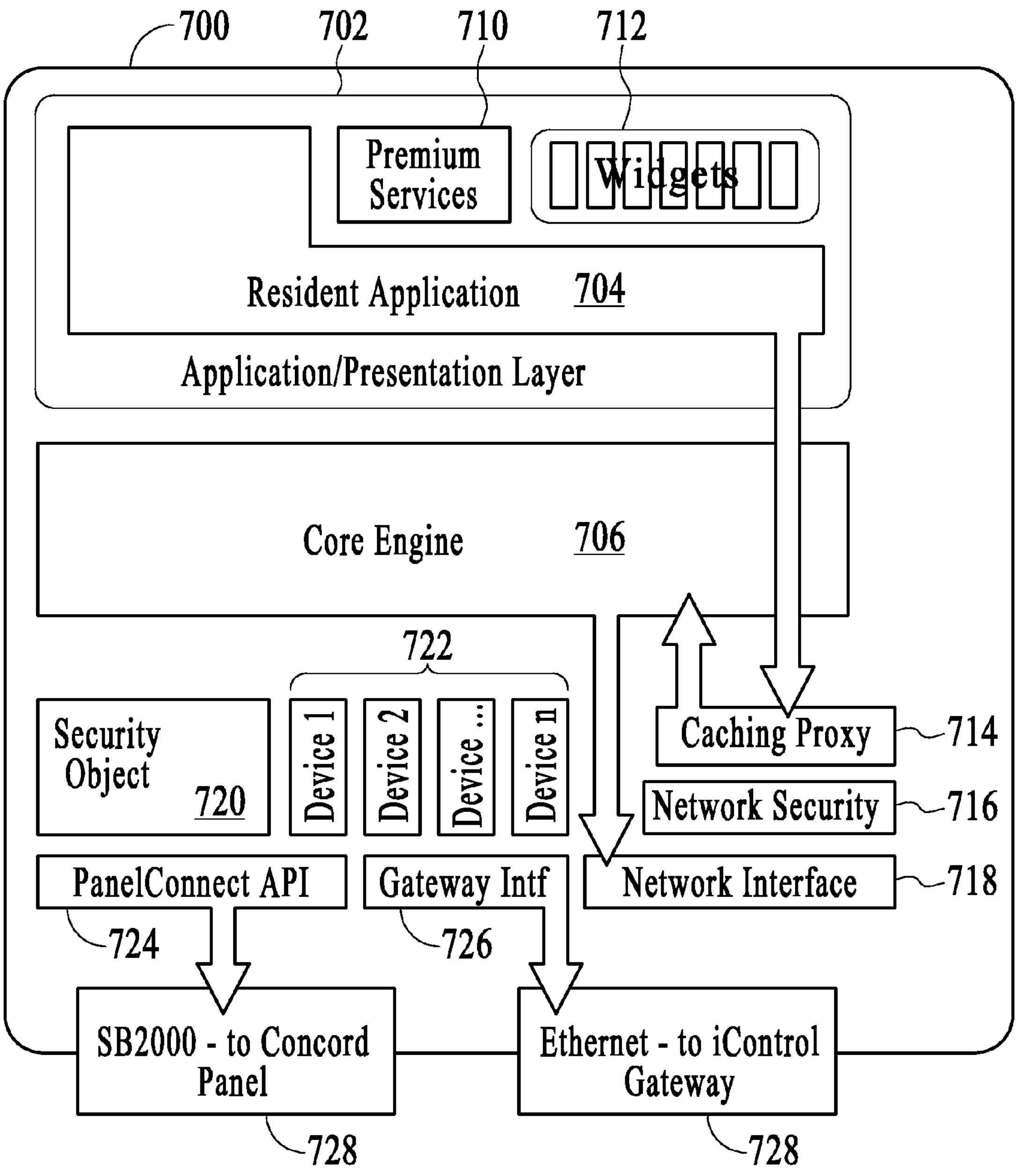

700
702
710
712
Premium Services
Widgets
Resident Application 704
Application/Presentation Layer
Core Engine 706
722
Security Object 720
Device 1
Device 2
Device ...
Device n
Caching Proxy
714
Network Security
716
PanelConnect API
Gateway Intf
Network Interface
718
724
726
SB2000 - to Concord Panel
Ethernet - to iControl Gateway
728
728

FIG.7

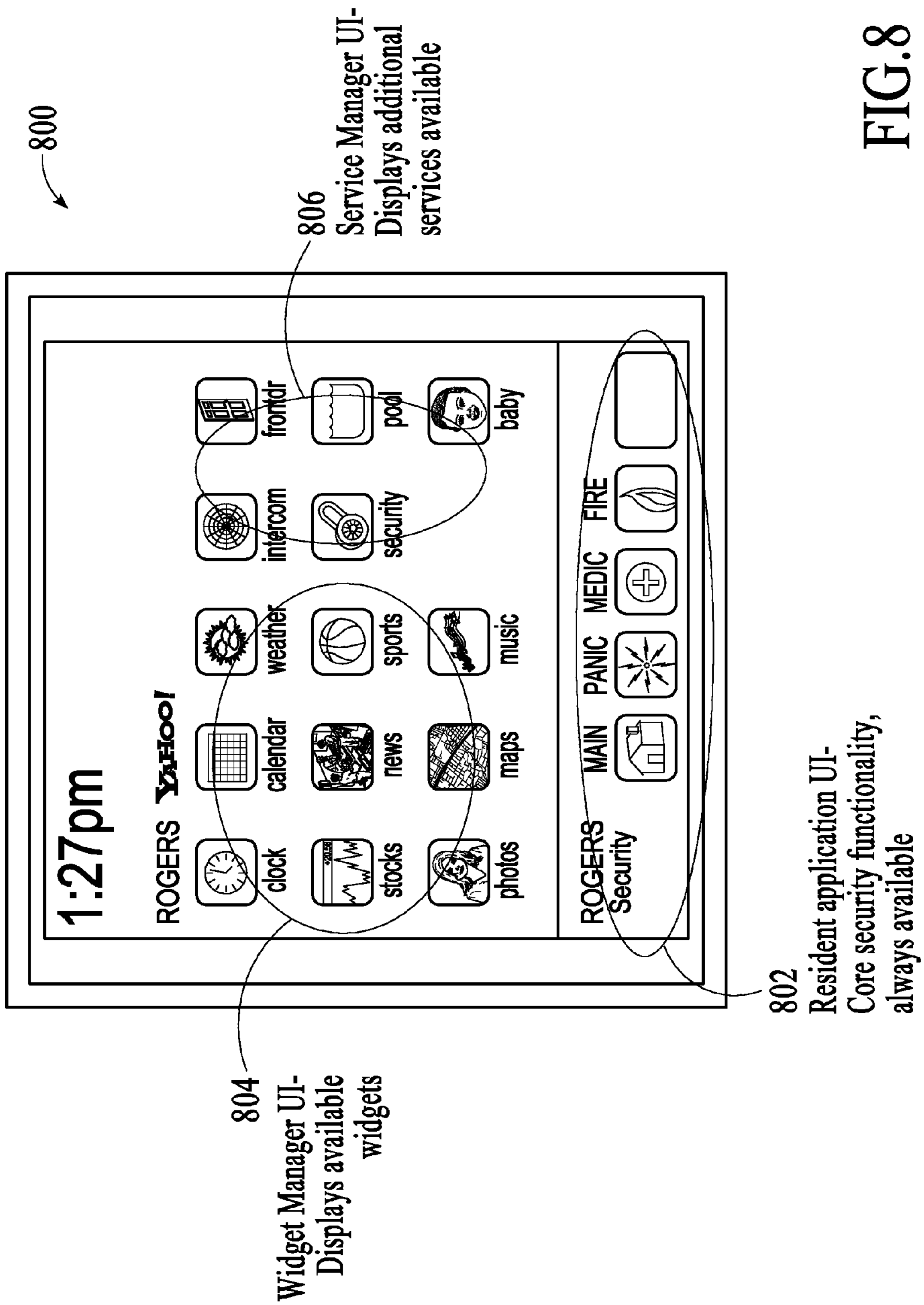

800
806
Service Manager UI-
Displays additional
services available
1:27pm
ROGERS YAHOO!
clock
calendar
weather
intercom
frontdr
stocks
news
sports
security
pool
photos
maps
music
baby
ROGERS
Security
MAIN
PANIC
MEDIC
FIRE
802
Resident application UI-
Core security functionality,
always available
804
Widget Manager UI-
Displays available
widgets

FIG.8

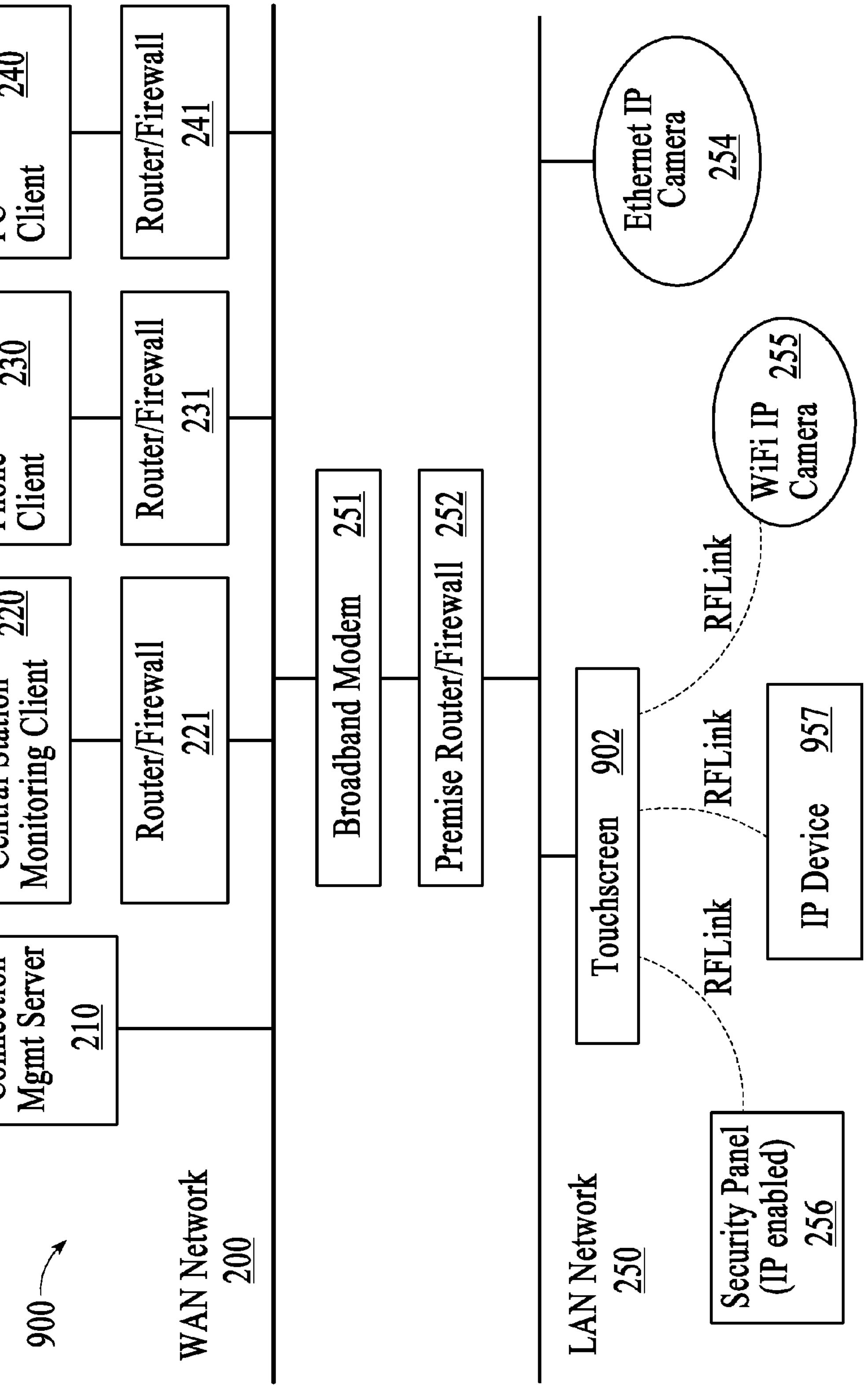
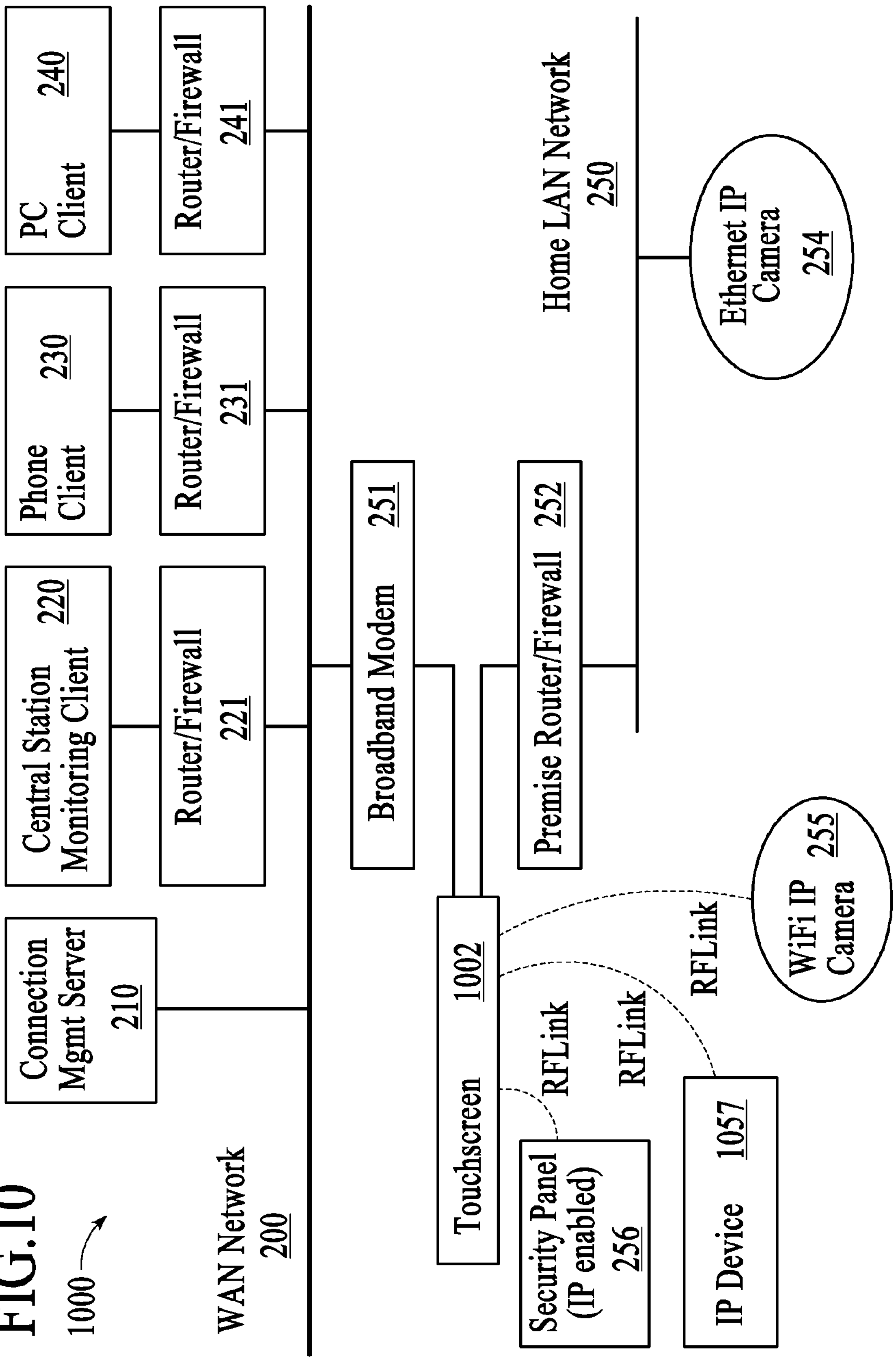

900
WAN Network 200
Connection Mgmt Server 210
Central Station Monitoring Client 220
Router/Firewall 221
Phone Client 230
Router/Firewall 231
PC Client 240
Router/Firewall 241
Broadband Modem 251
Premise Router/Firewall 252
LAN Network 250
Touchscreen 902
Ethernet IP Camera 254
WiFi IP Camera 255
IP Device 957
Security Panel (IP enabled) 256
RFLink
RFLink
RFLink

FIG.9

FIG.10


1000
WAN Network
200
Connection
Mgmt Server
210
Central Station
Monitoring Client
220
Router/Firewall
221
Phone
Client
230
Router/Firewall
231
PC
Client
240
Router/Firewall
241
Broadband Modem
251
Premise Router/Firewall
252
Home LAN Network
250
Ethernet IP
Camera
254
WiFi IP
Camera
255
Touchscreen
1002
RFLink
RFLink
RFLink
Security Panel
(IP enabled)
256
IP Device
1057

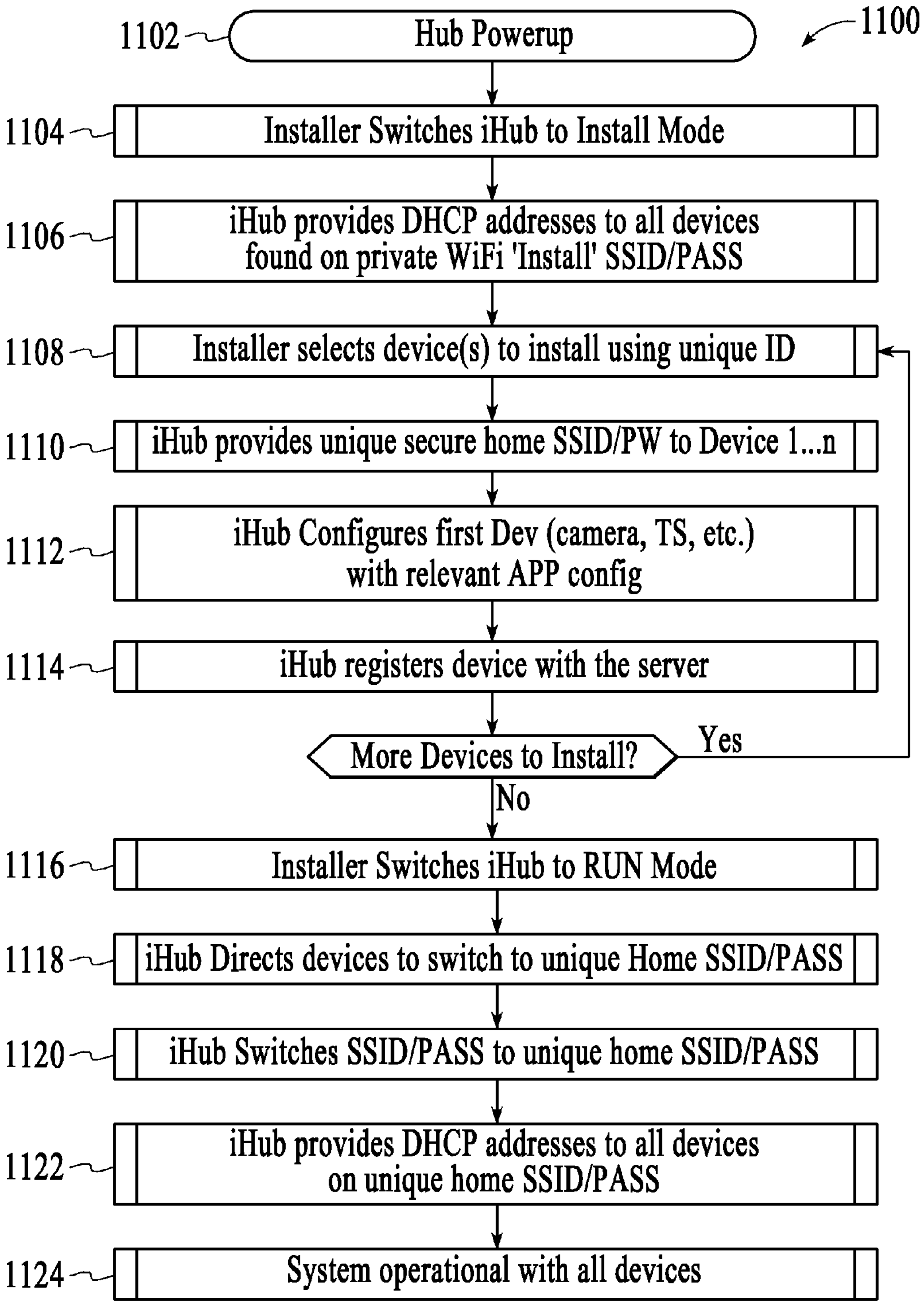

1100
1102
Hub Powerup
1104
Installer Switches iHub to Install Mode
1106
iHub provides DHCP addresses to all devices found on private WiFi 'Install' SSID/PASS
1108
Installer selects device(s) to install using unique ID
1110
iHub provides unique secure home SSID/PW to Device 1...n
1112
iHub Configures first Dev (camera, TS, etc.) with relevant APP config
1114
iHub registers device with the server
More Devices to Install?
Yes
No
1116
Installer Switches iHub to RUN Mode
1118
iHub Directs devices to switch to unique Home SSID/PASS
1120
iHub Switches SSID/PASS to unique home SSID/PASS
1122
iHub provides DHCP addresses to all devices on unique home SSID/PASS
1124
System operational with all devices

FIG.11

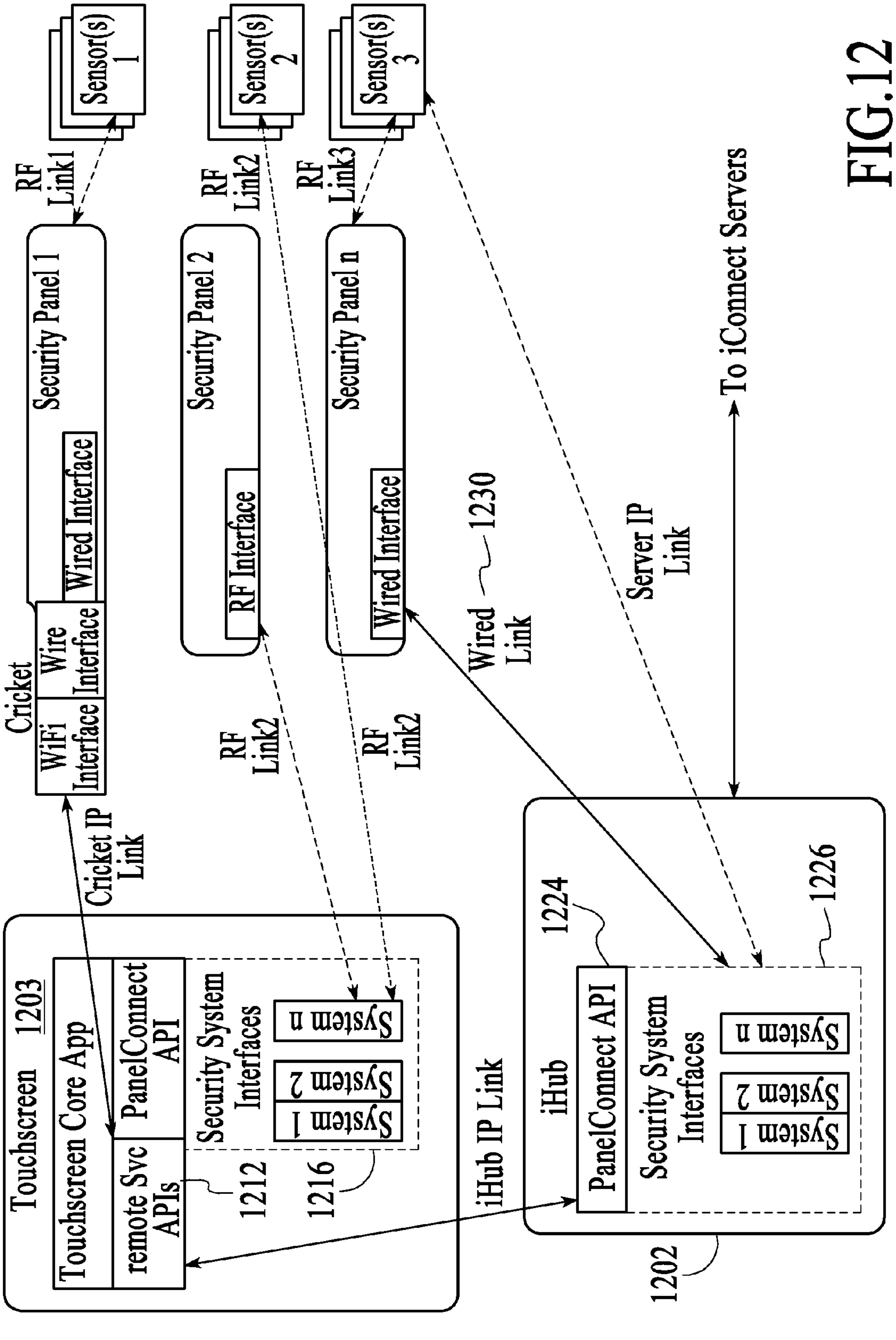

Touchscreen 1203
Touchscreen Core App
remote Svc APIs
PanelConnect API
Security System Interfaces
System 1
System 2
System n
1212
1216
Cricket IP Link
Cricket
WiFi Interface
Wire Interface
Wired Interface
Security Panel 1
RF Link1
Sensor(s) 1
Security Panel 2
RF Interface
RF Link2
Sensor(s) 2
Security Panel n
Wired Interface
RF Link3
Sensor(s) 3
RF Link2
RF Link2
Wired Link
1230
Server IP Link
To iConnect Servers
iHub IP Link
iHub
PanelConnect API
Security System Interfaces
System 1
System 2
System n
1224
1226
1202

FIG.12

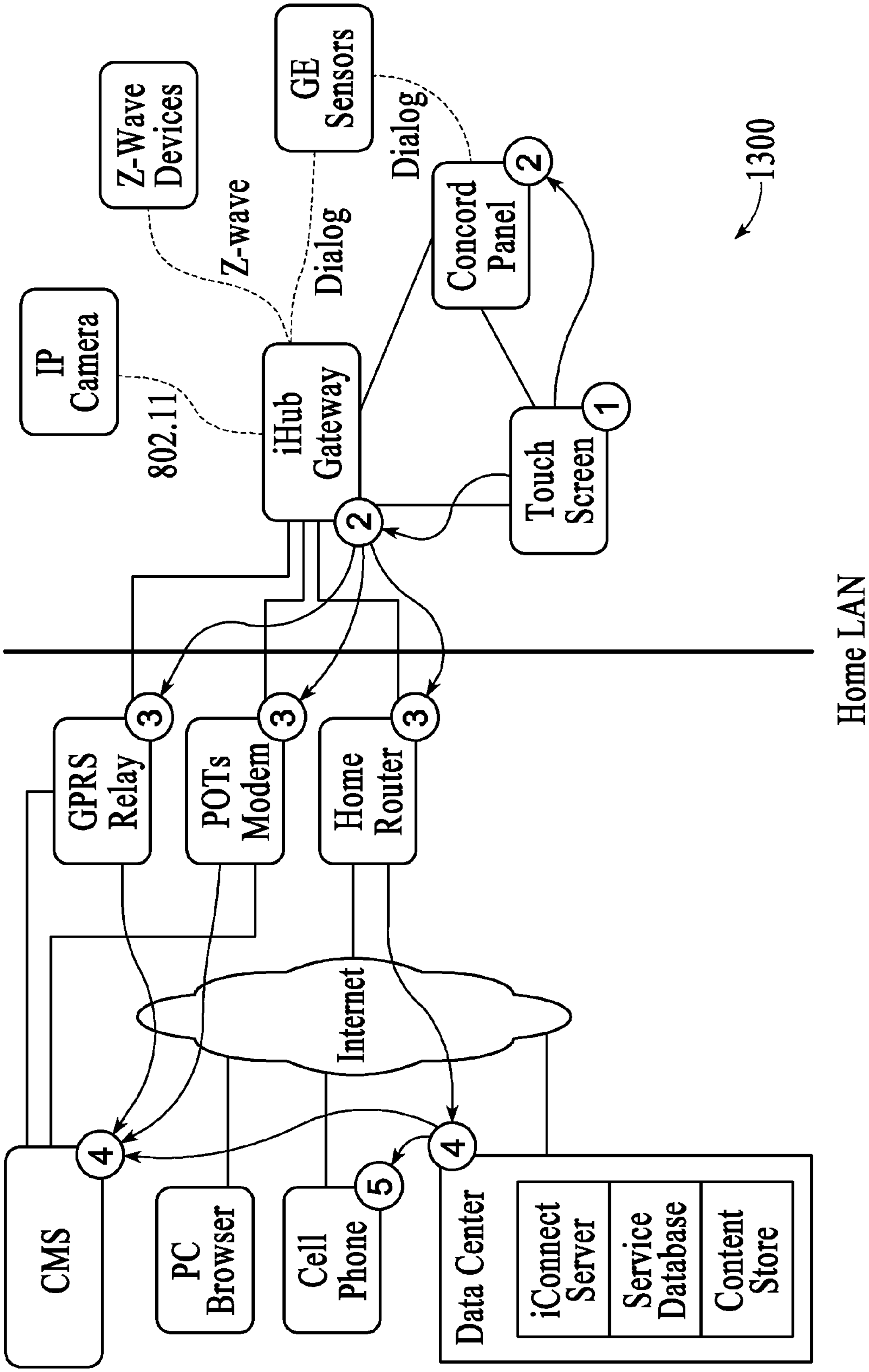

IP Camera
802.11
Z-Wave Devices
Z-wave
GE Sensors
Dialog
Dialog
iHub Gateway
Concord Panel
Touch Screen
1
2
2
3
3
3
Home LAN
GPRS Relay
POTs Modem
Home Router
Internet
4
4
5
CMS
PC Browser
Cell Phone
Data Center
iConnect Server
Service Database
Content Store
1300

FIG.13

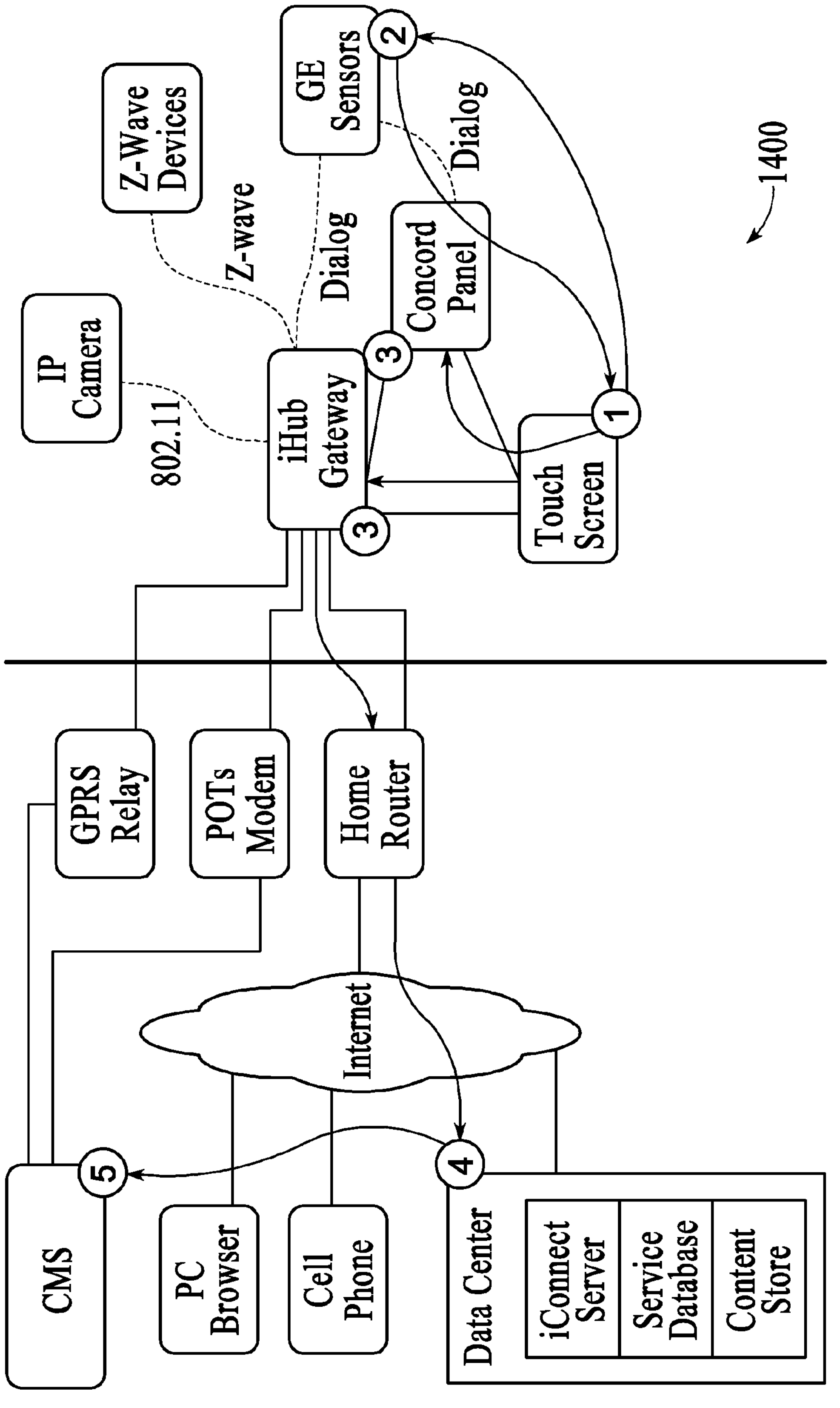

IP Camera
802.11
Z-Wave Devices
Z-wave
GE Sensors
Dialog
Dialog
Concord Panel
iHub Gateway
Touch Screen
1
2
3
3
1400
Home LAN
GPRS Relay
POTs Modem
Home Router
Internet
CMS
PC Browser
Cell Phone
Data Center
iConnect Server
Service Database
Content Store
4
5

FIG.14

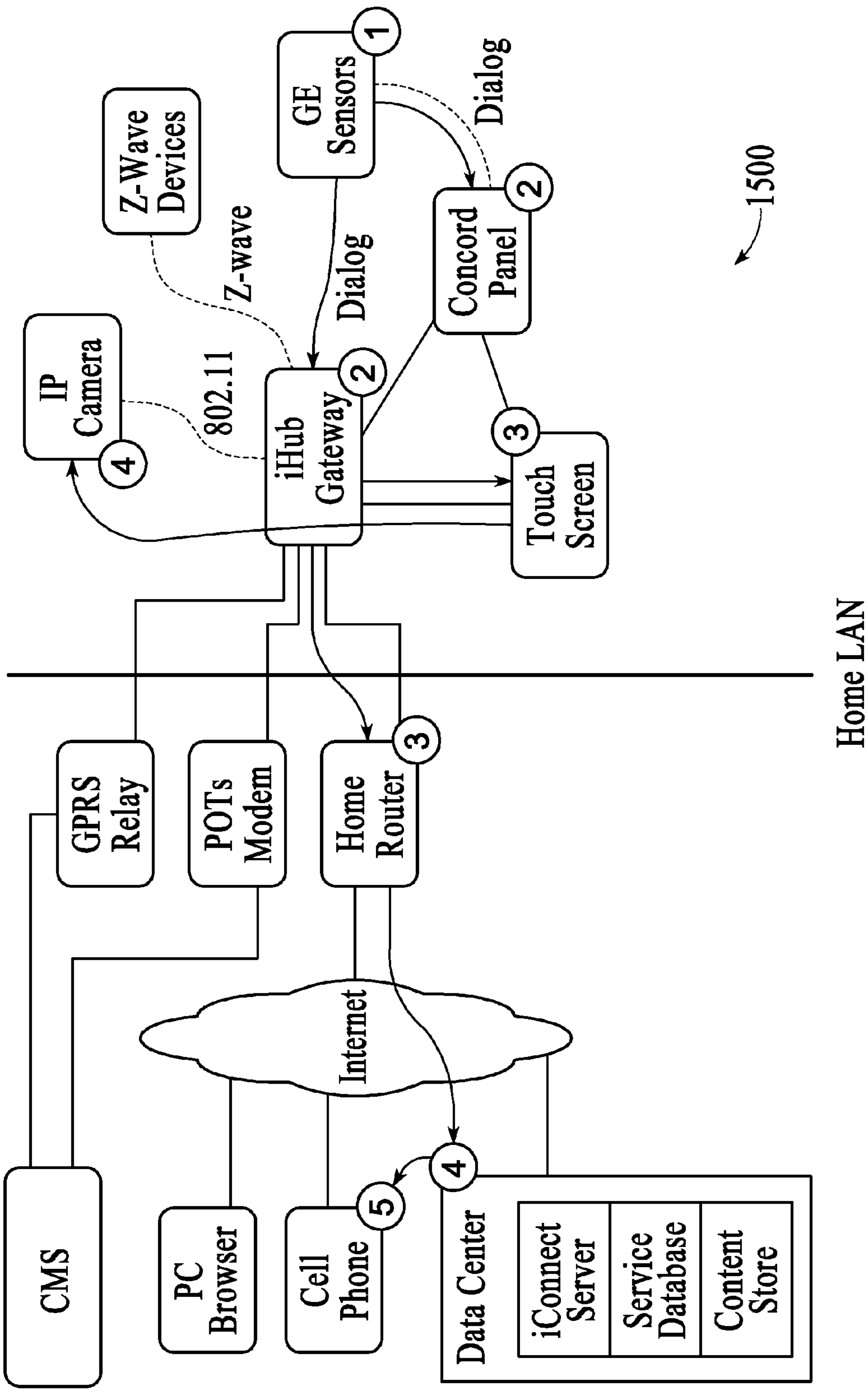

GE Sensors
1
Dialog
Z-Wave Devices
Z-wave
Dialog
Concord Panel
2
IP Camera
4
802.11
iHub Gateway
2
Touch Screen
3
Home LAN
GPRS Relay
POTs Modem
Home Router
3
Internet
CMS
PC Browser
Cell Phone
5
Data Center
4
iConnect Server
Service Database
Content Store
1500

FIG.15

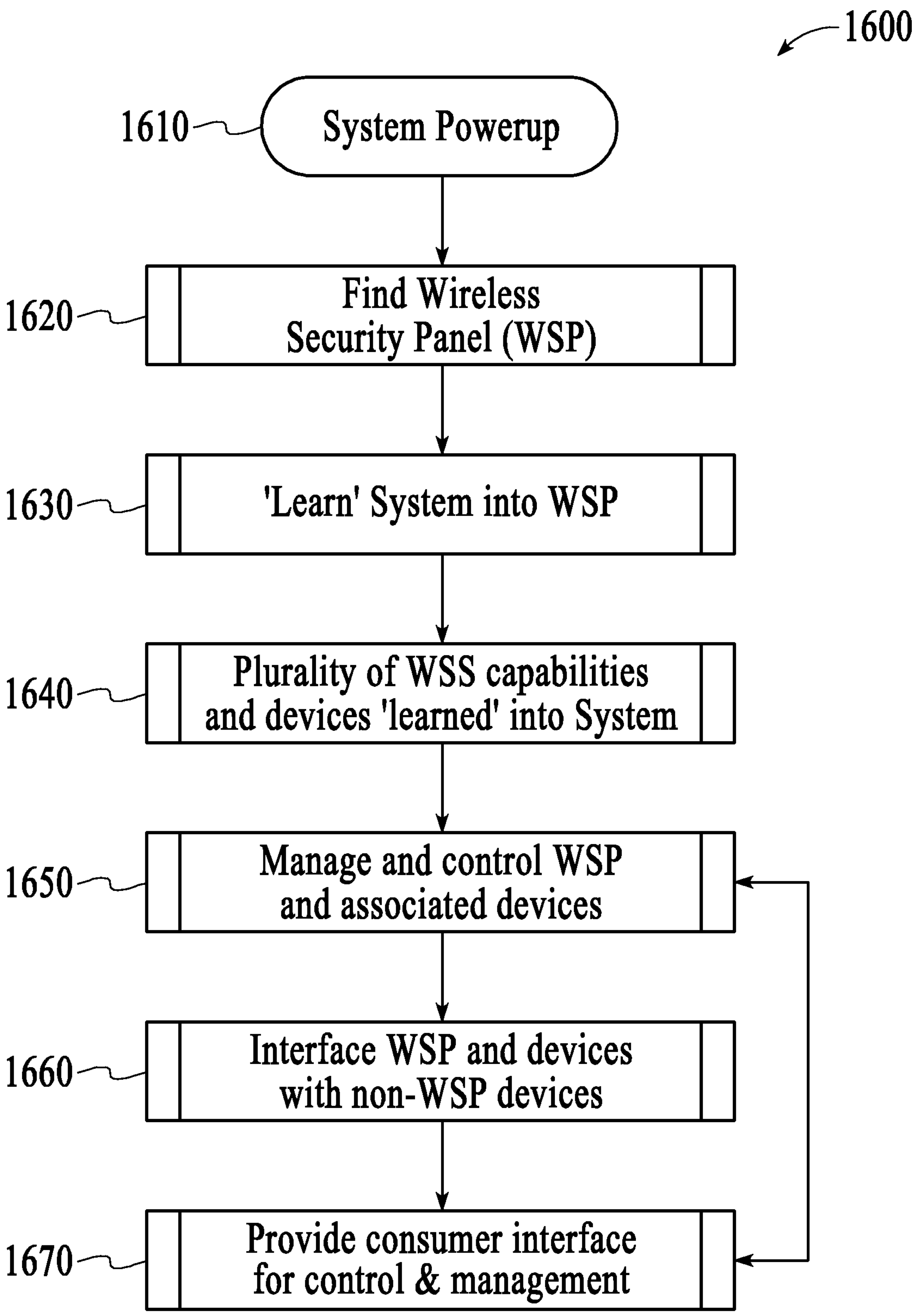
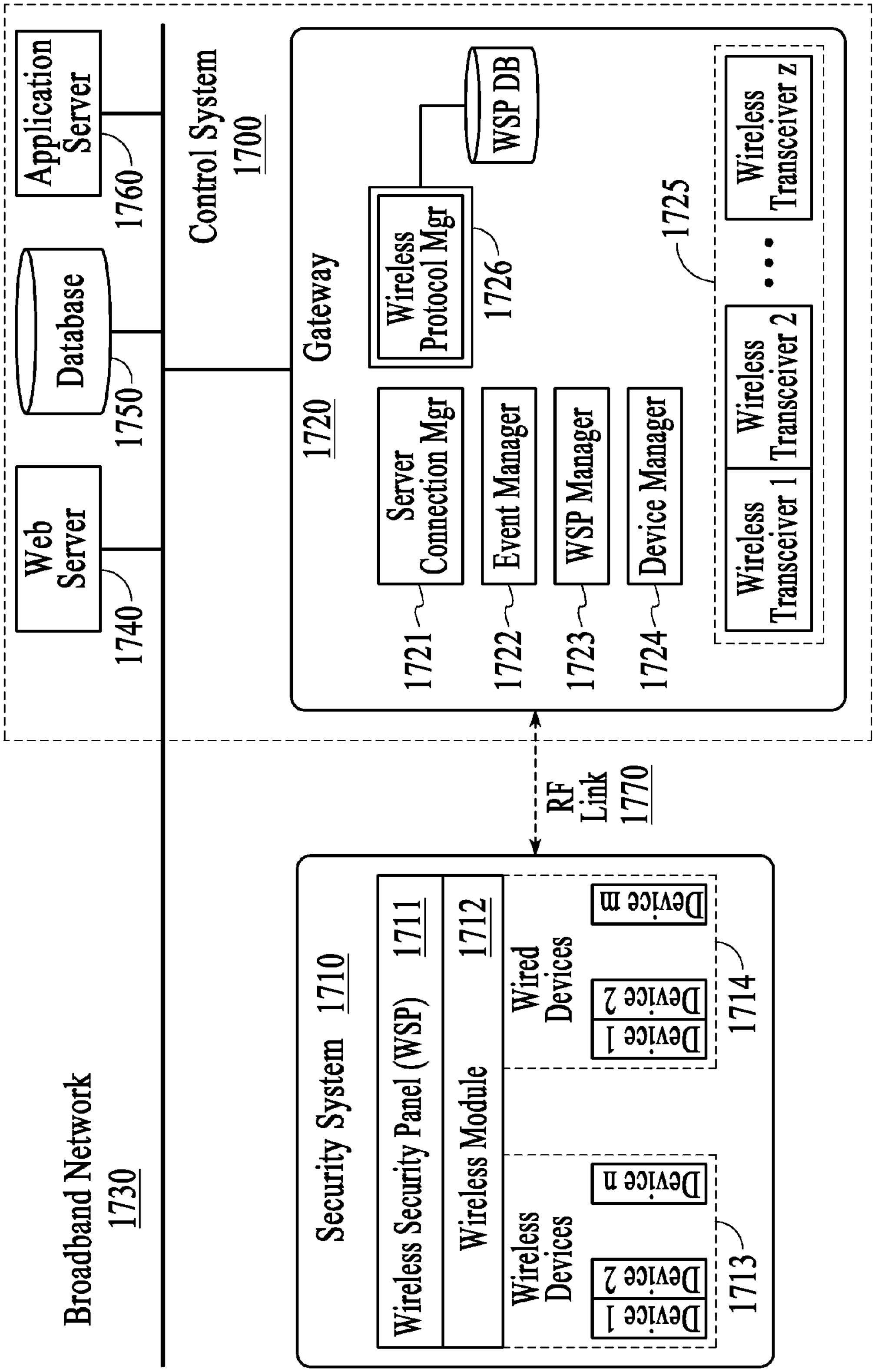

1600
1610
System Powerup
1620
Find Wireless Security Panel (WSP)
1630
'Learn' System into WSP
1640
Plurality of WSS capabilities and devices 'learned' into System
1650
Manage and control WSP and associated devices
1660
Interface WSP and devices with non-WSP devices
1670
Provide consumer interface for control & management

FIG.16



Application Server
1760
Database
1750
Web Server
1740
Control System
1700
Gateway
1720
WSP DB
Wireless Protocol Mgr
1726
Server Connection Mgr
1721
Event Manager
1722
WSP Manager
1723
Device Manager
1724
1725
Wireless Transceiver 1
Wireless Transceiver 2
Wireless Transceiver z
RF Link
1770
Broadband Network
1730
Security System 1710
Wireless Security Panel (WSP) 1711
Wireless Module 1712
Wireless Devices
Device 1
Device 2
Device n
1713
Wired Devices
Device 1
Device 2
Device m
1714

FIG.17

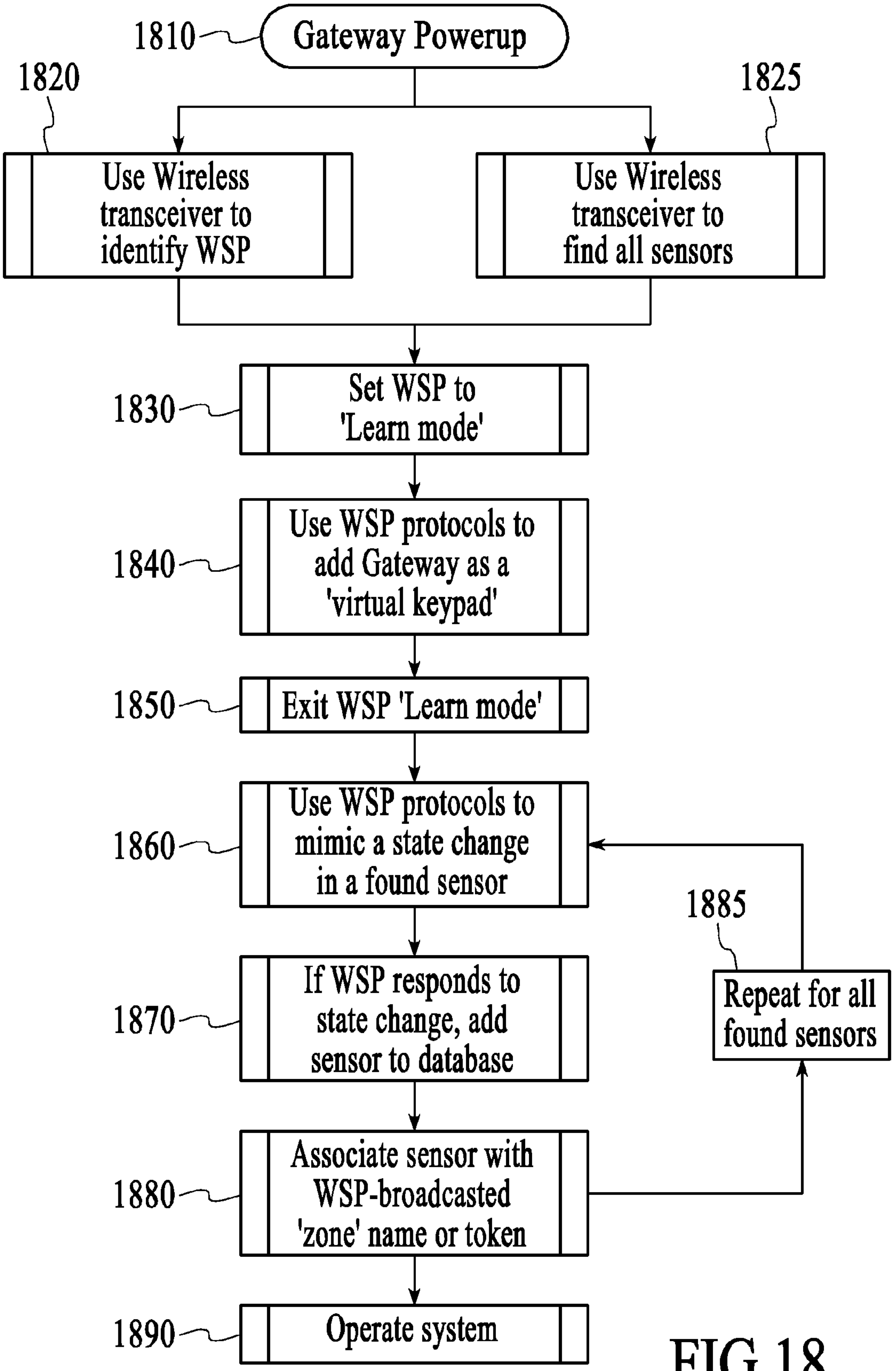

1810
Gateway Powerup
1820
Use Wireless transceiver to identify WSP
1825
Use Wireless transceiver to find all sensors
1830
Set WSP to 'Learn mode'
1840
Use WSP protocols to add Gateway as a 'virtual keypad'
1850
Exit WSP 'Learn mode'
1860
Use WSP protocols to mimic a state change in a found sensor
1870
If WSP responds to state change, add sensor to database
1880
Associate sensor with WSP-broadcasted 'zone' name or token
1885
Repeat for all found sensors
1890
Operate system

FIG.18

SECURITY SYSTEM WITH NETWORKED TOUCHSCREEN

RELATED APPLICATIONS

This application claims the benefit of U.S. Patent Application No. 60/957,997, filed Aug. 24, 2007.

This application claims the benefit of U.S. Patent Application No. 60/968,005, filed Aug. 24, 2007.

This application claims the benefit of U.S. Patent Application No. 60/987,359, filed Nov. 12, 2007.

This application claims the benefit of U.S. Patent Application No. 60/987,366, filed Nov. 12, 2007.

This application claims the benefit of U.S. Patent Application No. 61/019,162, filed Jan. 4, 2008.

This application claims the benefit of U.S. Patent Application No. 61/019,167, filed Jan. 4, 2008.

This application claims the benefit of U.S. Patent Application No. 61/023,489, filed Jan. 25, 2008.

This application claims the benefit of U.S. Patent Application No. 61/023,493, filed Jan. 25, 2008.

This application claims the benefit of U.S. Patent Application No. 61/023,496, filed Jan. 25, 2008.

This application claims the benefit of U.S. Patent Application No. 61/087,967, filed Aug. 11, 2008.

This application is a continuation in part application of U.S. patent application Ser. No. 11/084,232, filed Mar. 16, 2005.

This application is a continuation in part application of U.S. patent application Ser. No. 11/761,718, filed Jun. 12, 2007.

This application is a continuation in part application of U.S. patent application Ser. No. 11/761,745, filed Jun. 12, 2007.

This application is a continuation in part application of U.S. patent application Ser. No. 12/019,554, filed Jan. 24, 2008.

This application is a continuation in part application of U.S. patent application Ser. No. 12/019,568, filed Jan. 24, 2008.

This application is a continuation in part application of U.S. patent application Ser. No. 12/189,757, filed Aug. 11, 2008.

TECHNICAL FIELD

The embodiments described herein relate generally to a method and apparatus for improving the capabilities of security systems in home and business applications. More particularly, the embodiments described herein relate to a touchscreen device that integrates security system control and functionality with network content interactivity, management and presentation.

BACKGROUND

The field of home and small business security is dominated by technology suppliers who build comprehensive 'closed' security systems, where the individual components (sensors, security panels, keypads) operate solely within the confines of a single vendor solution. For example, a wireless motion sensor from vendor A cannot be used with a security panel from vendor B. Each vendor typically has developed sophisticated proprietary wireless technologies to enable the installation and management of wireless sensors, with little or no ability for the wireless devices to operate separate from the vendor's homogeneous system. Furthermore, these traditional systems are extremely limited in their ability to interface either to a local or wide area standards-based network (such as an IP network); most installed systems support only a low-bandwidth, intermittent connection utilizing phone lines or cellular (RF) backup systems. Wireless security technology from providers such as GE Security, Honeywell, and DSC/Tyco are well known in the art, and are examples of this proprietary approach to security systems for home and business.

Furthermore, with the proliferation of the internet, ethernet and WiFi local area networks (LANs) and advanced wide area networks (WANs) that offer high bandwidth, low latency connections (broadband), as well as more advanced wireless WAN data networks (e.g. GPRS or CDMA 1xRTT) there increasingly exists the networking capability to extend these traditional security systems to offer enhanced functionality. In addition, the proliferation of broadband access has driven a corresponding increase in home and small business networking technologies and devices. It is desirable to extend traditional security systems to encompass enhanced functionality such as the ability to control and manage security systems from the world wide web, cellular telephones, or advanced function internet-based devices. Other desired functionality includes an open systems approach to interface home security systems to home and small business networks.

Due to the proprietary approach described above, the traditional vendors are the only ones capable of taking advantage of these new network functions. To date, even though the vast majority of home and business customers have broadband network access in their premises, most security systems do not offer the advanced capabilities associated with high speed, low-latency LANs and WANs. This is primarily because the proprietary vendors have not been able to deliver such technology efficiently or effectively. Solution providers attempting to address this need are becoming known in the art, including three categories of vendors: traditional proprietary hardware providers such as Honeywell and GE Security; third party hard-wired module providers such as Alarm.com, NextAlarm, and uControl; and new proprietary systems providers such as InGrid.

A disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the continued proprietary approach of these vendors. As they develop technology in this area it once again operates only with the hardware from that specific vendor, ignoring the need for a heterogeneous, cross-vendor solution. Yet another disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the lack of experience and capability of these companies in creating open internet and web based solutions, and consumer friendly interfaces.

A disadvantage of the prior art technologies of the third party hard-wired module providers arises due to the installation and operational complexities and functional limitations associated with hardwiring a new component into existing security systems. Moreover, a disadvantage of the prior art technologies of the new proprietary systems providers arises due to the need to discard all prior technologies, and implement an entirely new form of security system to access the new functionalities associated with broadband and wireless data networks. There remains, therefore, a need for systems, devices, and methods that easily interface to and control the existing proprietary security technologies utilizing a variety of wireless technologies.

Incorporation by Reference

Each patent, patent application, and/or publication mentioned in this specification is herein incorporated by reference in its entirety to the same extent as if each individual patent, patent application, and/or publication was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of the integrated security system, under an embodiment.

FIG. **2** is a block diagram of components of the integrated security system, under an embodiment.

FIG. **3** is a block diagram of the gateway software or applications, under an embodiment.

FIG. **4** is a block diagram of the gateway components, under an embodiment.

FIG. **5** is a block diagram of IP device integration with a premise network, under an embodiment.

FIG. **6** is a block diagram of IP device integration with a premise network, under an alternative embodiment.

FIG. **7** is a block diagram of a touchscreen, under an embodiment.

FIG. **8** is an example screenshot of a networked security touchscreen, under an embodiment.

FIG. **9** is a block diagram of network or premise device integration with a premise network, under an embodiment.

FIG. **10** is a block diagram of network or premise device integration with a premise network, under an alternative embodiment.

FIG. **11** is a flow diagram for installation of an IP device into a private network environment, under an embodiment.

FIG. **12** is a block diagram showing communications among IP devices of the private network environment, under an embodiment.

FIG. **13** is a data flow diagram for a panic alarm, under an embodiment.

FIG. **14** is a data flow diagram for device installation, under an embodiment.

FIG. **15** is a data flow diagram for a camera event, under an embodiment.

FIG. **16** is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment.

FIG. **17** is a block diagram of an integrated security system wirelessly interfacing to proprietary security systems, under an embodiment.

FIG. **18** is a flow diagram for wirelessly 'learning' the gateway into an existing security system and discovering extant sensors, under an embodiment.

DETAILED DESCRIPTION

An integrated security system is described that integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network (broadband, cellular/GSM, POTS access) that enables users to remotely stay connected to their premises. The integrated security system, while delivering remote premise monitoring and control functionality to conventional monitored premise protection, complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices (cameras, lamp modules, thermostats, etc.) can be added, enabling users to remotely see live video and/or pictures and control home devices via their personal web portal or webpage, mobile phone, and/or other remote client device. Users can also receive notifications via email or text message when happenings occur, or do not occur, in their home.

Although the detailed description herein contains many specifics for the purposes of illustration, anyone of ordinary skill in the art will appreciate that many variations and alterations to the following details are within the scope of the embodiments described herein. Thus, the following illustrative embodiments are set forth without any loss of generality to, and without imposing limitations upon, the claimed invention.

In accordance with the embodiments described herein, a wireless system (e.g., radio frequency (RF)) is provided that enables a security provider or consumer to extend the capabilities of an existing RF-capable security system or a non-RF-capable security system that has been upgraded to support RF capabilities. The system includes an RF-capable Gateway device (physically located within RF range of the RF-capable security system) and associated software operating on the Gateway device. The system also includes a web server, application server, and remote database providing a persistent store for information related to the system.

The security systems of an embodiment, referred to herein as the iControl security system or integrated security system, extend the value of traditional home security by adding broadband access and the advantages of remote home monitoring and home control through the formation of a security network including components of the integrated security system integrated with a conventional premise security system and a premise local area network (LAN). With the integrated security system, conventional home security sensors, cameras, touchscreen keypads, lighting controls, and/or Internet Protocol (IP) devices in the home (or business) become connected devices that are accessible anywhere in the world from a web browser, mobile phone or through content-enabled touchscreens. The integrated security system experience allows security operators to both extend the value proposition of their monitored security systems and reach new consumers that include broadband users interested in staying connected to their family, home and property when they are away from home.

The integrated security system of an embodiment includes security servers (also referred to herein as iConnect servers or security network servers) and an iHub gateway (also referred to herein as the gateway, the iHub, or the iHub client) that couples or integrates into a home network (e.g., LAN) and communicates directly with the home security panel, in both wired and wireless installations. The security system of an embodiment automatically discovers the security system components (e.g., sensors, etc.) belonging to the security system and connected to a control panel of the security system and provides consumers with full two-way access via web and mobile portals. The gateway supports various wireless protocols and can interconnect with a wide range of control panels offered by security system providers. Service providers and users can then extend the system's capabilities with the additional IP cameras, lighting modules or security devices such as interactive touchscreen keypads. The integrated security system adds an enhanced value to these security systems by enabling consumers to stay connected through email and SMS alerts, photo push, event-based video capture and rule-based monitoring and notifications. This solution extends the reach of home security to households with broadband access.

The integrated security system builds upon the foundation afforded by traditional security systems by layering broadband and mobile access, IP cameras, interactive touchscreens, and an open approach to home automation on top of traditional security system configurations. The integrated security system is easily installed and managed by the security operator, and simplifies the traditional security installation process, as described below.

The integrated security system provides an open systems solution to the home security market. As such, the foundation of the integrated security system customer premises equipment (CPE) approach has been to abstract devices, and allows applications to manipulate and manage multiple devices from any vendor. The integrated security system DeviceConnect technology that enables this capability supports protocols, devices, and panels from GE Security and Honeywell, as well as consumer devices using Z-Wave, IP cameras (e.g., Ethernet, wifi, and Homeplug), and IP touchscreens. The DeviceConnect is a device abstraction layer that enables any device or protocol layer to interoperate with integrated security system components. This architecture enables the addition of new devices supporting any of these interfaces, as well as add entirely new protocols.

The benefit of DeviceConnect is that it provides supplier flexibility. The same consistent touchscreen, web, and mobile user experience operate unchanged on whatever security equipment selected by a security system provider, with the system provider's choice of IP cameras, backend data center and central station software.

The integrated security system provides a complete system that integrates or layers on top of a conventional host security system available from a security system provider. The security system provider therefore can select different components or configurations to offer (e.g., CDMA, GPRS, no cellular, etc.) as well as have iControl modify the integrated security system configuration for the system provider's specific needs (e.g., change the functionality of the web or mobile portal, add a GE or Honeywell-compatible TouchScreen, etc.).

The integrated security system integrates with the security system provider infrastructure for central station reporting directly via Broadband and GPRS alarm transmissions. Traditional dial-up reporting is supported via the standard panel connectivity. Additionally, the integrated security system provides interfaces for advanced functionality to the CMS, including enhanced alarm events, system installation optimizations, system test verification, video verification, 2-way voice over IP and GSM.

The integrated security system is an IP centric system that includes broadband connectivity so that the gateway augments the existing security system with broadband and GPRS connectivity. If broadband is down or unavailable GPRS may be used, for example. The integrated security system supports GPRS connectivity using an optional wireless package that includes a GPRS modem in the gateway. The integrated security system treats the GPRS connection as a higher cost though flexible option for data transfers. In an embodiment the GPRS connection is only used to route alarm events (e.g., for cost), however the gateway can be configured (e.g., through the iConnect server interface) to act as a primary channel and pass any or all events over GPRS. Consequently, the integrated security system does not interfere with the current plain old telephone service (POTS) security panel interface. Alarm events can still be routed through POTS; however the gateway also allows such events to be routed through a broadband or GPRS connection as well. The integrated security system provides a web application interface to the CSR tool suite as well as XML web services interfaces for programmatic integration between the security system provider's existing call center products. The integrated security system includes, for example, APIs that allow the security system provider to integrate components of the integrated security system into a custom call center interface. The APIs include XML web service APIs for integration of existing security system provider call center applications with the integrated security system service. All functionality available in the CSR Web application is provided with these API sets. The Java and XML-based APIs of the integrated security system support provisioning, billing, system administration, CSR, central station, portal user interfaces, and content management functions, to name a few. The integrated security system can provide a customized interface to the security system provider's billing system, or alternatively can provide security system developers with APIs and support in the integration effort.

The integrated security system provides or includes business component interfaces for provisioning, administration, and customer care to name a few. Standard templates and examples are provided with a defined customer professional services engagement to help integrate OSS/BSS systems of a Service Provider with the integrated security system.

The integrated security system components support and allow for the integration of customer account creation and deletion with a security system. The iConnect APIs provides access to the provisioning and account management system in iConnect and provide full support for account creation, provisioning, and deletion. Depending on the requirements of the security system provider, the iConnect APIs can be used to completely customize any aspect of the integrated security system backend operational system.

The integrated security system includes a gateway that supports the following standards-based interfaces, to name a few: Ethernet IP communications via Ethernet ports on the gateway, and standard XML/TCP/IP protocols and ports are employed over secured SSL sessions; USB 2.0 via ports on the gateway; 802.11b/g/n IP communications; GSM/GPRS RF WAN communications; CDMA 1xRTT RF WAN communications (optional, can also support EVDO and 3G technologies).

The gateway supports the following proprietary interfaces, to name a few: interfaces including Dialog RF network (319.5 MHz) and RS485 Superbus 2000 wired interface; RF mesh network (908 MHz); and interfaces including RF network (345 MHz) and RS485/RS232bus wired interfaces.

Regarding security for the IP communications (e.g., authentication, authorization, encryption, anti-spoofing, etc), the integrated security system uses SSL to encrypt all IP traffic, using server and client-certificates for authentication, as well as authentication in the data sent over the SSL-encrypted channel. For encryption, integrated security system issues public/private key pairs at the time/place of manufacture, and certificates are not stored in any online storage in an embodiment.

The integrated security system does not need any special rules at the customer premise and/or at the security system provider central station because the integrated security system makes outgoing connections using TCP over the standard HTTP and HTTPS ports. Provided outbound TCP connections are allowed then no special requirements on the firewalls are necessary.

FIG. **1** is a block diagram of the integrated security system **100**, under an embodiment. The integrated security system **100** of an embodiment includes the gateway **102** and the security servers **104** coupled to the conventional home security system **110**. At a customer's home or business, the gateway **102** connects and manages the diverse variety of home security and self-monitoring devices. The gateway **102** communicates with the iConnect Servers **104** located in the service provider's data center **106** (or hosted in integrated security system data center), with the communication taking place via a communication network **108** or other network (e.g., cellular network, internet, etc.). These servers **104** manage the system integrations necessary to deliver the integrated system service described herein. The combination of the gateway **102** and the iConnect servers **104** enable a wide variety of remote client devices **120** (e.g., PCs, mobile phones and PDAs) allowing users to remotely stay in touch with their home, business and family. In addition, the technology allows home security and self-monitoring information, as well as relevant third party content such as traffic and weather, to be presented in intuitive ways within the home, such as on advanced touchscreen keypads.

The integrated security system service (also referred to as iControl service) can be managed by a service provider via browser-based Maintenance and Service Management applications that are provided with the iConnect Servers. Or, if desired, the service can be more tightly integrated with existing OSS/BSS and service delivery systems via the iConnect web services-based XML APIs.

The integrated security system service can also coordinate the sending of alarms to the home security Central Monitoring Station (CMS) **199**. Alarms are passed to the CMS **199** using standard protocols such as Contact ID or SIA and can be generated from the home security panel location as well as by iConnect server **104** conditions (such as lack of communications with the integrated security system). In addition, the link between the security servers **104** and CMS **199** provides tighter integration between home security and self-monitoring devices and the gateway **102**. Such integration enables advanced security capabilities such as the ability for CMS personnel to view photos taken at the time a burglary alarm was triggered. For maximum security, the gateway **102** and iConnect servers **104** support the use of a mobile network (both GPRS and CDMA options are available) as a backup to the primary broadband connection.

The integrated security system service is delivered by hosted servers running software components that communicate with a variety of client types while interacting with other systems. FIG. **2** is a block diagram of components of the integrated security system **100**, under an embodiment. Following is a more detailed description of the components.

The iConnect servers **104** support a diverse collection of clients **120** ranging from mobile devices, to PCs, to in-home security devices, to a service provider's internal systems. Most clients **120** are used by end-users, but there are also a number of clients **120** that are used to operate the service.

Clients **120** used by end-users of the integrated security system **100** include, but are not limited to, the following:

- Clients based on gateway client applications **202** (e.g., a processor-based device running the gateway technology that manages home security and automation devices).
- A web browser **204** accessing a Web Portal application, performing end-user configuration and customization of the integrated security system service as well as monitoring of in-home device status, viewing photos and video, etc. Device and user management can also be performed by this portal application.
- A mobile device **206** (e.g., PDA, mobile phone, etc.) accessing the integrated security system Mobile Portal. This type of client **206** is used by end-users to view system status and perform operations on devices (e.g., turning on a lamp, arming a security panel, etc.) rather than for system configuration tasks such as adding a new device or user.
- PC or browser-based "widget" containers **208** that present integrated security system service content, as well as other third-party content, in simple, targeted ways (e.g. a widget that resides on a PC desktop and shows live video from a single in-home camera). "Widget" as used herein means applications or programs in the system.
- Touchscreen home security keypads **208** and advanced in-home devices that present a variety of content widgets via an intuitive touchscreen user interface.
- Notification recipients **210** (e.g., cell phones that receive SMS-based notifications when certain events occur (or don't occur), email clients that receive an email message with similar information, etc.).
- Custom-built clients (not shown) that access the iConnect web services XML API to interact with users' home security and self-monitoring information in new and unique ways. Such clients could include new types of mobile devices, or complex applications where integrated security system content is integrated into a broader set of application features.

In addition to the end-user clients, the iConnect servers **104** support PC browser-based Service Management clients that manage the ongoing operation of the overall service. These clients run applications that handle tasks such as provisioning, service monitoring, customer support and reporting.

There are numerous types of server components of the iConnect servers **104** of an embodiment including, but not limited to, the following: Business Components which manage information about all of the home security and self-monitoring devices; End-User Application Components which display that information for users and access the Business Components via published XML APIs; and Service Management Application Components which enable operators to administer the service (these components also access the Business Components via the XML APIs, and also via published SNMP MIBs).

The server components provide access to, and management of, the objects associated with an integrated security system installation. The top-level object is the "network." It is a location where a gateway **102** is located, and is also commonly referred to as a site or premises; the premises can include any type of structure (e.g., home, office, warehouse, etc.) at which a gateway **102** is located. Users can only access the networks to which they have been granted permission. Within a network, every object monitored by the gateway **102** is called a device. Devices include the sensors, cameras, home security panels and automation devices, as well as the controller or processor-based device running the gateway applications.

Various types of interactions are possible between the objects in a system. Automations define actions that occur as a result of a change in state of a device. For example, take a picture with the front entry camera when the front door sensor changes to "open". Notifications are messages sent to users to indicate that something has occurred, such as the front door going to "open" state, or has not occurred (referred to as an iWatch notification). Schedules define changes in device states that are to take place at predefined days and times. For example, set the security panel to "Armed" mode every weeknight at 11:00 pm.

The iConnect Business Components are responsible for orchestrating all of the low-level service management activities for the integrated security system service. They define all of the users and devices associated with a network (site), analyze how the devices interact, and trigger associated actions (such as sending notifications to users). All changes in device states are monitored and logged. The Business Components also manage all interactions with external systems as required, including sending alarms and other related self-monitoring data to the home security Central Monitoring System (CMS) **199**. The Business Components are implemented as portable Java J2EE Servlets, but are not so limited.

The following iConnect Business Components manage the main elements of the integrated security system service, but the embodiment is not so limited:

- A Registry Manager **220** defines and manages users and networks. This component is responsible for the creation, modification and termination of users and networks. It is also where a user's access to networks is defined.
- A Network Manager **222** defines and manages security and self-monitoring devices that are deployed on a network (site). This component handles the creation, modification, deletion and configuration of the devices, as well as the creation of automations, schedules and notification rules associated with those devices.
- A Data Manager **224** manages access to current and logged state data for an existing network and its devices. This component specifically does not provide any access to network management capabilities, such as adding new devices to a network, which are handled exclusively by the Network Manager **222**.
- To achieve optimal performance for all types of queries, data for current device states is stored separately from historical state data (a.k.a. "logs") in the database. A Log Data Manager **226** performs ongoing transfers of current device state data to the historical data log tables.

Additional iConnect Business Components handle direct communications with certain clients and other systems, for example:

- An iHub Manager **228** directly manages all communications with gateway clients, including receiving information about device state changes, changing the configuration of devices, and pushing new versions of the gateway client to the hardware it is running on.
- A Notification Manager **230** is responsible for sending all notifications to clients via SMS (mobile phone messages), email (via a relay server like an SMTP email server), etc.
- An Alarm and CMS Manager **232** sends critical server-generated alarm events to the home security Central Monitoring Station (CMS) and manages all other communications of integrated security system service data to and from the CMS.
- The Element Management System (EMS) **234** is an iControl Business Component that manages all activities associated with service installation, scaling and monitoring, and filters and packages service operations data for use by service management applications. The SNMP MIBs published by the EMS can also be incorporated into any third party monitoring system if desired.

The iConnect Business Components store information about the objects that they manage in the iControl Service Database **240** and in the iControl Content Store **242**. The iControl Content Store is used to store media objects like video, photos and widget content, while the Service Database stores information about users, networks, and devices. Database interaction is performed via a JDBC interface. For security purposes, the Business Components manage all data storage and retrieval.

The iControl Business Components provide web services-based APIs that application components use to access the Business Components' capabilities. Functions of application components include presenting integrated security system service data to end-users, performing administrative duties, and integrating with external systems and back-office applications.

The primary published APIs for the iConnect Business Components include, but are not limited to, the following:

- A Registry Manager API **252** provides access to the Registry Manager Business Component's functionality, allowing management of networks and users.
- A Network Manager API **254** provides access to the Network Manager Business Component's functionality, allowing management of devices on a network.
- A Data Manager API **256** provides access to the Data Manager Business Component's functionality, such as setting and retrieving (current and historical) data about device states.
- A Provisioning API **258** provides a simple way to create new networks and configure initial default properties.

Each API of an embodiment includes two modes of access: Java API or XML API. The XML APIs are published as web services so that they can be easily accessed by applications or servers over a network. The Java APIs are a programmer-friendly wrapper for the XML APIs. Application components and integrations written in Java should generally use the Java APIs rather than the XML APIs directly.

The iConnect Business Components also have an XML-based interface **260** for quickly adding support for new devices to the integrated security system. This interface **260**, referred to as DeviceConnect **260**, is a flexible, standards-based mechanism for defining the properties of new devices and how they can be managed. Although the format is flexible enough to allow the addition of any type of future device, pre-defined XML profiles are currently available for adding common types of devices such as sensors (SensorConnect), home security panels (PanelConnect) and IP cameras (CameraConnect).

The iConnect End-User Application Components deliver the user interfaces that run on the different types of clients supported by the integrated security system service. The components are written in portable Java J2EE technology (e.g., as Java Servlets, as JavaServer Pages (JSPs), etc.) and they all interact with the iControl Business Components via the published APIs.

The following End-User Application Components generate CSS-based HTML/JavaScript that is displayed on the target client. These applications can be dynamically branded with partner-specific logos and URL links (such as Customer Support, etc.). The End-User Application Components of an embodiment include, but are not limited to, the following:

- An iControl Activation Application **270** that delivers the first application that a user sees when they set up the integrated security system service. This wizard-based web browser application securely associates a new user with a purchased gateway and the other devices included with it as a kit (if any). It primarily uses functionality published by the Provisioning API.
- An iControl Web Portal Application **272** runs on PC browsers and delivers the web-based interface to the integrated security system service. This application allows users to manage their networks (e.g. add devices and create automations) as well as to view/change device states, and manage pictures and videos. Because of the wide scope of capabilities of this application, it uses three different Business Component APIs that include the Registry Manager API, Network Manager API, and Data Manager API, but the embodiment is not so limited.
- An iControl Mobile Portal **274** is a small-footprint web-based interface that runs on mobile phones and PDAs.

This interface is optimized for remote viewing of device states and pictures/videos rather than network management. As such, its interaction with the Business Components is primarily via the Data Manager API.

Custom portals and targeted client applications can be provided that leverage the same Business Component APIs used by the above applications.

A Content Manager Application Component **276** delivers content to a variety of clients. It sends multimedia-rich user interface components to widget container clients (both PC and browser-based), as well as to advanced touchscreen keypad clients. In addition to providing content directly to end-user devices, the Content Manager **276** provides widget-based user interface components to satisfy requests from other Application Components such as the iControl Web **272** and Mobile **274** portals.

A number of Application Components are responsible for overall management of the service. These pre-defined applications, referred to as Service Management Application Components, are configured to offer off-the-shelf solutions for production management of the integrated security system service including provisioning, overall service monitoring, customer support, and reporting, for example. The Service Management Application Components of an embodiment include, but are not limited to, the following:

A Service Management Application **280** allows service administrators to perform activities associated with service installation, scaling and monitoring/alerting. This application interacts heavily with the Element Management System (EMS) Business Component to execute its functionality, and also retrieves its monitoring data from that component via protocols such as SNMP MIBs.

A Kitting Application **282** is used by employees performing service provisioning tasks. This application allows home security and self-monitoring devices to be associated with gateways during the warehouse kitting process.

A CSR Application and Report Generator **284** is used by personnel supporting the integrated security system service, such as CSRs resolving end-user issues and employees enquiring about overall service usage. Pushes of new gateway firmware to deployed gateways is also managed by this application.

The iConnect servers **104** also support custom-built integrations with a service provider's existing OSS/BSS, CSR and service delivery systems **290**. Such systems can access the iConnect web services XML API to transfer data to and from the iConnect servers **104**. These types of integrations can compliment or replace the PC browser-based Service Management applications, depending on service provider needs.

As described above, the integrated security system of an embodiment includes a gateway, or iHub. The gateway of an embodiment includes a device that is deployed in the home or business and couples or connects the various third-party cameras, home security panels, sensors and devices to the iConnect server over a WAN connection as described in detail herein. The gateway couples to the home network and communicates directly with the home security panel in both wired and wireless sensor installations. The gateway is configured to be low-cost, reliable and thin so that it complements the integrated security system network-based architecture.

The gateway supports various wireless protocols and can interconnect with a wide range of home security control panels. Service providers and users can then extend the system's capabilities by adding IP cameras, lighting modules and additional security devices. The gateway is configurable to be integrated into many consumer appliances, including set-top boxes, routers and security panels. The small and efficient footprint of the gateway enables this portability and versatility, thereby simplifying and reducing the overall cost of the deployment.

FIG. **3** is a block diagram of the gateway **102** including gateway software or applications, under an embodiment. The gateway software architecture is relatively thin and efficient, thereby simplifying its integration into other consumer appliances such as set-top boxes, routers, touch screens and security panels. The software architecture also provides a high degree of security against unauthorized access. This section describes the various key components of the gateway software architecture.

The gateway application layer **302** is the main program that orchestrates the operations performed by the gateway. The Security Engine **304** provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine **304** of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.

Bi-directional authentication between the gateway and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.

Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The gateway provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.

802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.

A gateway-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying gateway-enabled devices have the knowledge that only a gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

A Remote Firmware Download module **306** allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server **104**, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Gateway firmware can be remotely download either for one gateway at a time, a group of gateways, or in batches.

The Automations engine **308** manages the user-defined rules of interaction between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

DeviceConnect **310** includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module **310** offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect **312** is provided for adding new sensors, CameraConnect **316** for adding IP cameras, and PanelConnect **314** for adding home security panels.

The Schedules engine **318** is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8 am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application. The Schedules Engine **318** then interfaces with SensorConnect **312** to ensure that scheduled events occur at precisely the desired time.

The Device Management module **320** is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters—to simplify the user experience and reduce the customer support burden, the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

The video routing engine **322** is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

FIG. **4** is a block diagram of components of the gateway **102**, under an embodiment. Depending on the specific set of functionality desired by the service provider deploying the integrated security system service, the gateway **102** can use any of a number of processors **402**, due to the small footprint of the gateway application firmware. In an embodiment, the gateway could include the Broadcom BCM5354 as the processor for example. In addition, the gateway **102** includes memory (e.g., FLASH **404**, RAM **406**, etc.) and any number of input/output (I/O) ports **408**.

Referring to the WAN portion **410** of the gateway **102**, the gateway **102** of an embodiment can communicate with the iConnect server using a number of communication types and/or protocols, for example Broadband **412**, GPRS **414** and/or Public Switched Telephone Network (PTSN) **416** to name a few. In general, broadband communication **412** is the primary means of connection between the gateway **102** and the iConnect server **104** and the GPRS/CDMA **414** and/or PSTN **416** interfaces acts as back-up for fault tolerance in case the user's broadband connection fails for whatever reason, but the embodiment is not so limited.

Referring to the LAN portion **420** of the gateway **102**, various protocols and physical transceivers can be used to communicate to off-the-shelf sensors and cameras. The gateway **102** is protocol-agnostic and technology-agnostic and as such can easily support almost any device networking protocol. The gateway **102** can, for example, support GE and Honeywell security RF protocols **422**, Z-Wave **424**, serial (RS232 and RS485) **426** for direct connection to security panels as well as WiFi 428 (802.11b/g) for communication to WiFi cameras.

The integrated security system includes couplings or connections among a variety of IP devices or components, and the device management module is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system of an embodiment uses a "sandbox" network to discover and manage all IP devices coupled or connected as components of the system. The IP devices of an embodiment include wired devices, wireless devices, cameras, interactive touchscreens, and security panels to name a few. These devices can be wired via ethernet cable or Wifi devices, all of which are secured within the sandbox network, as described below. The "sandbox" network is described in detail below.

FIG. **5** is a block diagram **500** of network or premise device integration with a premise network **250**, under an embodiment. In an embodiment, network devices **255**-**257** are coupled to the gateway **102** using a secure network coupling or connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption). The network coupling or connection between the gateway **102** and the network devices **255**-**257** is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway **102** is coupled to the premise router/firewall **252** via a coupling with a premise LAN **250**. The premise router/firewall **252** is coupled to a broadband modem **251**, and the broadband modem **251** is coupled to a WAN **200** or other network outside the premise. The gateway **102** thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN **250** of the host premises. The gateway sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway **102** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the gateway **102**.

FIG. **6** is a block diagram **600** of network or premise device integration with a premise network **250**, under an alternative embodiment. The network or premise devices **255**-**257** are coupled to the gateway **102**. The network coupling or connection between the gateway **102** and the network devices **255**-**257** is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway **102** is coupled or connected between the premise router/firewall **252** and the broadband modem **251**. The broadband modem **251** is coupled to a WAN **200** or other network outside the premise, while the premise router/firewall **252** is coupled to a premise LAN **250**. As a result of its location between the broadband modem **251** and the premise router/firewall **252**, the gateway **102** can be configured or function as the premise router routing specified data between the outside network (e.g., WAN **200**) and the premise router/

firewall **252** of the LAN **250**. As described above, the gateway **102** in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices **255-257** and is coupled or connected between the LAN **250** of the host premises and the WAN **200**. The gateway sub-network can include, but is not limited to, any number of network or premise devices **255-257** like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway **102** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the gateway **102**.

The examples described above with reference to FIGS. **5** and **6** are presented only as examples of IP device integration. The integrated security system is not limited to the type, number and/or combination of IP devices shown and described in these examples, and any type, number and/or combination of IP devices is contemplated within the scope of this disclosure as capable of being integrated with the premise network.

The integrated security system of an embodiment includes a touchscreen (also referred to as the iControl touchscreen or integrated security system touchscreen), as described above, which provides core security keypad functionality, content management and presentation, and embedded systems design. The networked security touchscreen system of an embodiment enables a consumer or security provider to easily and automatically install, configure and manage the security system and touchscreen located at a customer premise. Using this system the customer may access and control the local security system, local IP devices such as cameras, local sensors and control devices (such as lighting controls or pipe freeze sensors), as well as the local security system panel and associated security sensors (such as door/window, motion, and smoke detectors). The customer premise may be a home, business, and/or other location equipped with a wired or wireless broadband IP connection.

The system of an embodiment includes a touchscreen with a configurable software user interface and/or a gateway device (e.g., iHub) that couples or connects to a premise security panel through a wired or wireless connection, and a remote server that provides access to content and information from the premises devices to a user when they are remote from the home. The touchscreen supports broadband and/or WAN wireless connectivity. In this embodiment, the touchscreen incorporates an IP broadband connection (e.g., Wifi radio, Ethernet port, etc.), and/or a cellular radio (e.g., GPRS/GSM, CDMA, WiMax, etc.). The touchscreen described herein can be used as one or more of a security system interface panel and a network user interface (UI) that provides an interface to interact with a network (e.g., LAN, WAN, internet, etc.).

The touchscreen of an embodiment provides an integrated touchscreen and security panel as an all-in-one device. Once integrated using the touchscreen, the touchscreen and a security panel of a premise security system become physically co-located in one device, and the functionality of both may even be co-resident on the same CPU and memory (though this is not required).

The touchscreen of an embodiment also provides an integrated IP video and touchscreen UI. As such, the touchscreen supports one or more standard video CODECs/players (e.g., H.264, Flash Video, MOV, MPEG4, M-JPEG, etc.). The touchscreen UI then provides a mechanism (such as a camera or video widget) to play video. In an embodiment the video is streamed live from an IP video camera. In other embodiments the video comprises video clips or photos sent from an IP camera or from a remote location.

The touchscreen of an embodiment provides a configurable user interface system that includes a configuration supporting use as a security touchscreen. In this embodiment, the touchscreen utilizes a modular user interface that allows components to be modified easily by a service provider, an installer, or even the end user. Examples of such a modular approach include using Flash widgets, HTML-based widgets, or other downloadable code modules such that the user interface of the touchscreen can be updated and modified while the application is running. In an embodiment the touchscreen user interface modules can be downloaded over the internet. For example, a new security configuration widget can be downloaded from a standard web server, and the touchscreen then loads such configuration app into memory, and inserts it in place of the old security configuration widget. The touchscreen of an embodiment is configured to provide a self-install user interface.

Embodiments of the networked security touchscreen system described herein include a touchscreen device with a user interface that includes a security toolbar providing one or more functions including arm, disarm, panic, medic, and alert. The touchscreen therefore includes at least one screen having a separate region of the screen dedicated to a security toolbar. The security toolbar of an embodiment is present in the dedicated region at all times that the screen is active.

The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing home-based functions. The home-based functions of an embodiment include managing, viewing, and/or controlling IP video cameras. In this embodiment, regions of the home screen are allocated in the form of widget icons; these widget icons (e.g. for cameras, thermostats, lighting, etc) provide functionality for managing home systems. So, for example, a displayed camera icon, when selected, launches a Camera Widget, and the Camera widget in turn provides access to video from one or more cameras, as well as providing the user with relevant camera controls (take a picture, focus the camera, etc.)

The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing, viewing, and/or controlling internet-based content or applications. For example, the Widget Manager UI presents a region of the home screen (up to and including the entire home screen) where internet widgets icons such as weather, sports, etc. may be accessed). Each of these icons may be selected to launch their respective content services.

The touchscreen of an embodiment is integrated into a premise network using the gateway, as described above. The gateway as described herein functions to enable a separate wireless network, or sub-network, that is coupled, connected, or integrated with another network (e.g., WAN, LAN of the host premises, etc.). The sub-network enabled by the gateway optimizes the installation process for IP devices, like the touchscreen, that couple or connect to the sub-network by segregating these IP devices from other such devices on the network. This segregation of the IP devices of the sub-network further enables separate security and privacy policies to be implemented for these IP devices so that, where the IP devices are dedicated to specific functions (e.g., security), the security and privacy policies can be tailored specifically for the specific functions. Furthermore, the gateway and the sub-network it forms enables the segregation of data traffic, resulting in faster and more efficient data flow between components of the host network, components of the sub-network, and between components of the sub-network and components of the network.

The touchscreen of an embodiment includes a core functional embedded system that includes an embedded operating system, required hardware drivers, and an open system interface to name a few. The core functional embedded system can be provided by or as a component of a conventional security system (e.g., security system available from GE Security). These core functional units are used with components of the integrated security system as described herein. Note that portions of the touchscreen description below may include reference to a host premise security system (e.g., GE security system), but these references are included only as an example and do not limit the touchscreen to integration with any particular security system.

As an example, regarding the core functional embedded system, a reduced memory footprint version of embedded Linux forms the core operating system in an embodiment, and provides basic TCP/IP stack and memory management functions, along with a basic set of low-level graphics primitives. A set of device drivers is also provided or included that offer low-level hardware and network interfaces. In addition to the standard drivers, an interface to the RS 485 bus is included that couples or connects to the security system panel (e.g., GE Concord panel). The interface may, for example, implement the Superbus 2000 protocol, which can then be utilized by the more comprehensive transaction-level security functions implemented in PanelConnect technology (e.g SetAlarmLevel (int level, int partition, char *accessCode)). Power control drivers are also provided.

FIG. **7** is a block diagram of a touchscreen **700** of the integrated security system, under an embodiment. The touchscreen **700** generally includes an application/presentation layer **702** with a resident application **704**, and a core engine **706**. The touchscreen **700** also includes one or more of the following, but is not so limited: applications of premium services **710**, widgets **712**, a caching proxy **714**, network security **716**, network interface **718**, security object **720**, applications supporting devices **722**, PanelConnect API **724**, a gateway interface **726**, and one or more ports **728**.

More specifically, the touchscreen, when configured as a home security device, includes but is not limited to the following application or software modules: RS 485 and/or RS-232 bus security protocols to conventional home security system panel (e.g., GE Concord panel); functional home security classes and interfaces (e.g. Panel ARM state, Sensor status, etc.); Application/Presentation layer or engine; Resident Application; Consumer Home Security Application; installer home security application; core engine; and System bootloader/Software Updater. The core Application engine and system bootloader can also be used to support other advanced content and applications. This provides a seamless interaction between the premise security application and other optional services such as weather widgets or IP cameras.

An alternative configuration of the touchscreen includes a first Application engine for premise security and a second Application engine for all other applications. The integrated security system application engine supports content standards such as HTML, XML, Flash, etc. and enables a rich consumer experience for all 'widgets', whether security-based or not. The touchscreen thus provides service providers the ability to use web content creation and management tools to build and download any 'widgets' regardless of their functionality.

As discussed above, although the Security Applications have specific low-level functional requirements in order to interface with the premise security system, these applications make use of the same fundamental application facilities as any other 'widget', application facilities that include graphical layout, interactivity, application handoff, screen management, and network interfaces, to name a few.

Content management in the touchscreen provides the ability to leverage conventional web development tools, performance optimized for an embedded system, service provider control of accessible content, content reliability in a consumer device, and consistency between 'widgets' and seamless widget operational environment. In an embodiment of the integrated security system, widgets are created by web developers and hosted on the integrated security system Content Manager (and stored in the Content Store database). In this embodiment the server component caches the widgets and offers them to consumers through the web-based integrated security system provisioning system. The servers interact with the advanced touchscreen using HTTPS interfaces controlled by the core engine and dynamically download widgets and updates as needed to be cached on the touchscreen. In other embodiments widgets can be accessed directly over a network such as the Internet without needing to go through the iControl Content Manager

Referring to FIG. **7**, the touchscreen system is built on a tiered architecture, with defined interfaces between the Application/Presentation Layer (the Application Engine) on the top, the Core Engine in the middle, and the security panel and gateway APIs at the lower level. The architecture is configured to provide maximum flexibility and ease of maintenance.

The application engine of the touchscreen provides the presentation and interactivity capabilities for all applications (widgets) that run on the touchscreen, including both core security function widgets and third party content widgets. FIG. **8** is an example screenshot **800** of a networked security touchscreen, under an embodiment. This example screenshot **800** includes three interfaces or user interface (UI) components **802-806**, but is not so limited. A first UI **802** of the touchscreen includes icons by which a user controls or accesses functions and/or components of the security system (e.g., "Main", "Panic", "Medic", "Fire", state of the premise alarm system (e.g., disarmed, armed, etc.), etc.); the first UI **802**, which is also referred to herein as a security interface, is always presented on the touchscreen. A second UI **804** of the touchscreen includes icons by which a user selects or interacts with services and other network content (e.g., clock, calendar, weather, stocks, news, sports, photos, maps, music, etc.) that is accessible via the touchscreen. The second UI **804** is also referred to herein as a network interface or content interface. A third UI **806** of the touchscreen includes icons by which a user selects or interacts with additional services or components (e.g., intercom control, security, cameras coupled to the system in particular regions (e.g., front door, baby, etc.) available via the touchscreen.

A component of the application engine is the Presentation Engine, which includes a set of libraries that implement the standards-based widget content (e.g., XML, HTML, JavaScript, Flash) layout and interactivity. This engine provides the widget with interfaces to dynamically load both graphics and application logic from third parties, support high level data description language as well as standard graphic formats. The set of web content-based functionality available to a widget developer is extended by specific touchscreen functions implemented as local web services by the Core Engine.

The resident application of the touchscreen is the master service that controls the interaction of all widgets in the system, and enforces the business and security rules required by the service provider. For example, the resident application determines the priority of widgets, thereby enabling a home security widget to override resource requests from a less critical widget (e.g. a weather widget). The resident application also monitors widget behavior, and responds to client or server requests for cache updates.

The core engine of the touchscreen manages interaction with other components of the integrated security system, and provides an interface through which the resident application and authorized widgets can get information about the home security system, set alarms, install sensors, etc. At the lower level, the Core Engine's main interactions are through the PanelConnect API, which handles all communication with the security panel, and the gateway Interface, which handles communication with the gateway. In an embodiment, both the iHub Interface and PanelConnect API are resident and operating on the touchscreen. In another embodiment, the PanelConnect API runs on the gateway or other device that provides security system interaction and is accessed by the touchscreen through a web services interface.

The Core Engine also handles application and service level persistent and cached memory functions, as well as the dynamic provisioning of content and widgets, including but not limited to: flash memory management, local widget and content caching, widget version management (download, cache flush new/old content versions), as well as the caching and synchronization of user preferences. As a portion of these services the Core engine incorporates the bootloader functionality that is responsible for maintaining a consistent software image on the touchscreen, and acts as the client agent for all software updates. The bootloader is configured to ensure full update redundancy so that unsuccessful downloads cannot corrupt the integrated security system.

Video management is provided as a set of web services by the Core Engine. Video management includes the retrieval and playback of local video feeds as well as remote control and management of cameras (all through iControl CameraConnect technology).

Both the high level application layer and the mid-level core engine of the touchscreen can make calls to the network. Any call to the network made by the application layer is automatically handed off to a local caching proxy, which determines whether the request should be handled locally. Many of the requests from the application layer are web services API requests; although such requests could be satisfied by the iControl servers, they are handled directly by the touchscreen and the gateway. Requests that get through the caching proxy are checked against a white list of acceptable sites, and, if they match, are sent off through the network interface to the gateway. Included in the Network Subsystem is a set of network services including HTTP, HTTPS, and server-level authentication functions to manage the secure client-server interface. Storage and management of certificates is incorporated as a part of the network services layer.

Server components of the integrated security system servers support interactive content services on the touchscreen. These server components include, but are not limited to the content manager, registry manager, network manager, and global registry, each of which is described herein.

The Content Manager oversees aspects of handling widget data and raw content on the touchscreen. Once created and validated by the service provider, widgets are 'ingested' to the Content Manager, and then become available as downloadable services through the integrated security system Content Management APIs. The Content manager maintains versions and timestamp information, and connects to the raw data contained in the backend Content Store database. When a widget is updated (or new content becomes available) all clients registering interest in a widget are systematically updated as needed (a process that can be configured at an account, locale, or system-wide level).

The Registry Manager handles user data, and provisioning accounts, including information about widgets the user has decided to install, and the user preferences for these widgets.

The Network Manager handles getting and setting state for all devices on the integrated security system network (e.g., sensors, panels, cameras, etc.). The Network manager synchronizes with the gateway, the advanced touchscreen, and the subscriber database.

The Global Registry is a primary starting point server for all client services, and is a logical referral service that abstracts specific server locations/addresses from clients (touchscreen, gateway **102**, desktop widgets, etc.). This approach enables easy scaling/migration of server farms.

The touchscreen of an embodiment operates wirelessly with a premise security system. The touchscreen of an embodiment incorporates an RF transceiver component that either communicates directly with the sensors and/or security panel over the panel's proprietary RF frequency, or the touchscreen communicates wirelessly to the gateway over 802.11, Ethernet, or other IP-based communications channel, as described in detail herein. In the latter case the gateway implements the PanelConnect interface and communicates directly to the security panel and/or sensors over wireless or wired networks as described in detail above.

The touchscreen of an embodiment is configured to operate with multiple security systems through the use of an abstracted security system interface. In this embodiment, the PanelConnect API can be configured to support a plurality of proprietary security system interfaces, either simultaneously or individually as described herein. In one embodiment of this approach, the touchscreen incorporates multiple physical interfaces to security panels (e.g. GE Security RS-485, Honeywell RF, etc.) in addition to the PanelConnect API implemented to support multiple security interfaces. The change needed to support this in PanelConnect is a configuration parameter specifying the panel type connection that is being utilized.

So for example, the setARMState( ) function is called with an additional parameter (e.g., Armstate=setARMState (type="ARM STAY|ARM AWAY|DISARM", Parameters="ExitDelay=30 |Lights=OFF", panelType="GE Concord4 RS485")). The 'panelType' parameter is used by the setARMState function (and in practice by all of the PanelConnect functions) to select an algorithm appropriate to the specific panel out of a plurality of alogorithms.

The touchscreen of an embodiment is self-installable. Consequently, the touchscreen provides a 'wizard' approach similar to that used in traditional computer installations (e.g. InstallShield). The wizard can be resident on the touchscreen, accessible through a web interface, or both. In one embodiment of a touchscreen self-installation process, the service provider can associate devices (sensors, touchscreens, security panels, lighting controls, etc.) remotely using a web-based administrator interface.

The touchscreen of an embodiment includes a battery backup system for a security touchscreen. The touchscreen incorporates a standard Li-ion or other battery and charging circuitry to allow continued operation in the event of a power outage. In an embodiment the battery is physically located and connected within the touchscreen enclosure. In another embodiment the battery is located as a part of the power transformer, or in between the power transformer and the touchscreen.

The example configurations of the integrated security system described above with reference to FIGS. **5** and **6** include a gateway that is a separate device, and the touchscreen couples to the gateway. However, in an alternative embodiment, the gateway device and its functionality can be incorporated into the touchscreen so that the device management module, which is now a component of or included in the touchscreen, is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system with the integrated touchscreen/gateway uses the same "sandbox" network to discover and manage all IP devices coupled or connected as components of the system.

The touchscreen of this alternative embodiment integrates the components of the gateway with the components of the touchscreen as described herein. More specifically, the touchscreen of this alternative embodiment includes software or applications described above with reference to FIG. **3**. In this alternative embodiment, the touchscreen includes the gateway application layer **302** as the main program that orchestrates the operations performed by the gateway. A Security Engine **304** of the touchscreen provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine **304** of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

- Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.
- Bi-directional authentication between the touchscreen and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.
- Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The touchscreen provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.
- 802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.
- A touchscreen-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying touchscreen-enabled devices have the knowledge that only a gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

A Remote Firmware Download module **306** of the touchscreen allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server **104**, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Touchscreen firmware can be remotely download either for one touchscreen at a time, a group of touchscreen, or in batches.

The Automations engine **308** of the touchscreen manages the user-defined rules of interaction between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

DeviceConnect **310** of the touchscreen touchscreen includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module **310** offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect **312** is provided for adding new sensors, CameraConnect **316** for adding IP cameras, and PanelConnect **314** for adding home security panels.

The Schedules engine **318** of the touchscreen is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8 am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application of the touchscreen. The Schedules Engine **318** then interfaces with SensorConnect **312** to ensure that scheduled events occur at precisely the desired time.

The Device Management module **320** of the touchscreen is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters, and the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

The video routing engine **322** of the touchscreen is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

FIG. **9** is a block diagram **900** of network or premise device integration with a premise network **250**, under an embodiment. In an embodiment, network devices **255**, **256**, **957** are coupled to the touchscreen **902** using a secure network connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption), and the touchscreen **902** coupled to the premise router/firewall **252** via a coupling with a premise LAN **250**. The premise router/firewall **252** is coupled to a broadband modem **251**, and the broadband modem **251** is coupled to a WAN **200** or other network outside the premise. The touchscreen **902** thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN **250** of the host premises. The touchscreen sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and IP devices, to name a few. The touchscreen **902** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the touchscreen **902**.

FIG. **10** is a block diagram **1000** of network or premise device integration with a premise network **250**, under an alternative embodiment. The network or premise devices **255**, **256**, **1057** are coupled to the touchscreen **1002**, and the touchscreen **1002** is coupled or connected between the premise router/firewall **252** and the broadband modem **251**. The broadband modem **251** is coupled to a WAN **200** or other network outside the premise, while the premise router/firewall **252** is coupled to a premise LAN **250**. As a result of its location between the broadband modem **251** and the premise router/firewall **252**, the touchscreen **1002** can be configured or function as the premise router routing specified data between the outside network (e.g., WAN **200**) and the premise router/firewall **252** of the LAN **250**. As described above, the touchscreen **1002** in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices **255**, **156**, **1057** and is coupled or connected between the LAN **250** of the host premises and the WAN **200**. The touchscreen sub-network can include, but is not limited to, any number of network or premise devices **255**, **256**, **1057** like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The touchscreen **1002** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the touchscreen **1002**.

The gateway of an embodiment, whether a stand-along component or integrated with a touchscreen, enables couplings or connections and thus the flow or integration of information between various components of the host premises and various types and/or combinations of IP devices, where the components of the host premises include a network (e.g., LAN) and/or a security system or subsystem to name a few. Consequently, the gateway controls the association between and the flow of information or data between the components of the host premises. For example, the gateway of an embodiment forms a sub-network coupled to another network (e.g., WAN, LAN, etc.), with the sub-network including IP devices. The gateway further enables the association of the IP devices of the sub-network with appropriate systems on the premises (e.g., security system, etc.). Therefore, for example, the gateway can form a sub-network of IP devices configured for security functions, and associate the sub-network only with the premises security system, thereby segregating the IP devices dedicated to security from other IP devices that may be coupled to another network on the premises.

In an example embodiment, FIG. **11** is a flow diagram **1100** for integration or installation of an IP device into a private network environment, under an embodiment. The IP device includes any IP-capable device which, for example, includes the touchscreen of an embodiment. The variables of an embodiment set at time of installation include, but are not limited to, one or more of a private SSID/Password, a gateway identifier, a security panel identifier, a user account TS, and a Central Monitoring Station account identification.

An embodiment of the IP device discovery and management begins with a user or installer activating **1102** the gateway and initiating **1104** the install mode of the system. This places the gateway in an install mode. Once in install mode, the gateway shifts to a default (Install) Wifi configuration. This setting will match the default setting for other integrated security system-enabled devices that have been pre-configured to work with the integrated security system. The gateway will then begin to provide **1106** DHCP addresses for these IP devices. Once the devices have acquired a new DHCP address from the gateway, those devices are available for configuration into a new secured Wifi network setting.

The user or installer of the system selects **1108** all devices that have been identified as available for inclusion into the integrated security system. The user may select these devices by their unique IDs via a web page, Touchscreen, or other client interface. The gateway provides **1110** data as appropriate to the devices. Once selected, the devices are configured **1112** with appropriate secured Wifi settings, including SSID and WPA/WPA-2 keys that are used once the gateway switches back to the secured sandbox configuration from the "Install" settings. Other settings are also configured as appropriate for that type of device. Once all devices have been configured, the user is notified and the user can exit install mode. At this point all devices will have been registered **1114** with the integrated security system servers.

The installer switches **1116** the gateway to an operational mode, and the gateway instructs or directs **1118** all newly configured devices to switch to the "secured" Wifi sandbox settings. The gateway then switches **1120** to the "secured" Wifi settings. Once the devices identify that the gateway is active on the "secured" network, they request new DHCP addresses from the gateway which, in response, provides **1122** the new addresses. The devices with the new addresses are then operational **1124** on the secured network.

In order to ensure the highest level of security on the secured network, the gateway can create or generate a dynamic network security configuration based on the unique ID and private key in the gateway, coupled with a randomizing factor that can be based on online time or other inputs. This guarantees the uniqueness of the gateway secured network configuration.

To enable the highest level of performance, the gateway analyzes the RF spectrum of the 802.11x network and determines which frequency band/channel it should select to run.

An alternative embodiment of the camera/IP device management process leverages the local ethernet connection of the sandbox network on the gateway. This alternative process is similar to the Wifi discovery embodiment described above, except the user connects the targeted device to the ethernet port of the sandbox network to begin the process. This alternative embodiment accommodates devices that have not been pre-configured with the default "Install" configuration for the integrated security system.

This alternative embodiment of the IP device discovery and management begins with the user/installer placing the system into install mode. The user is instructed to attach an IP device to be installed to the sandbox Ethernet port of the gateway. The IP device requests a DHCP address from the gateway which, in response to the request, provides the address. The user is presented the device and is asked if he/she wants to install the device. If yes, the system configures the device with the secured Wifi settings and other device-specific settings (e.g., camera settings for video length, image quality etc.). The user is next instructed to disconnect the device from the ethernet port. The device is now available for use on the secured sandbox network.

FIG. **12** is a block diagram showing communications among integrated IP devices of the private network environment, under an embodiment. The IP devices of this example include a security touchscreen **1203**, gateway **1202** (e.g., "iHub"), and security panel (e.g., "Security Panel **1**", "Security Panel **2**", "Security Panel n"), but the embodiment is not so limited. In alternative embodiments any number and/or combination of these three primary component types may be combined with other components including IP devices and/or security system components. For example, a single device which comprises an integrated gateway, touchscreen, and security panel is merely another embodiment of the integrated security system described herein. The description that follows includes an example configuration that includes a touchscreen hosting particular applications. However, the embodiment is not limited to the touchscreen hosting these applications, and the touchscreen should be thought of as representing any IP device.

Referring to FIG. **12**, the touchscreen **1203** incorporates an application **1210** that is implemented as computer code resident on the touchscreen operating system, or as a web-based application running in a browser, or as another type of scripted application (e.g., Flash, Java, Visual Basic, etc.). The touchscreen core application **1210** represents this application, providing user interface and logic for the end user to manage their security system or to gain access to networked information or content (Widgets). The touchscreen core application **1210** in turn accesses a library or libraries of functions to control the local hardware (e.g. screen display, sound, LEDs, memory, etc.) as well as specialized librarie(s) to couple or connect to the security system.

In an embodiment of this security system connection, the touchscreen **1203** communicates to the gateway **1202**, and has no direct communication with the security panel. In this embodiment, the touchscreen core application **1210** accesses the remote service APIs **1212** which provide security system functionality (e.g. ARM/DISARM panel, sensor state, get/set panel configuration parameters, initiate or get alarm events, etc.). In an embodiment, the remote service APIs **1212** implement one or more of the following functions, but the embodiment is not so limited: Armstate=setARMState(type="ARM STAY|ARM AWAY|DISARM", Parameters="ExitDelay=30 |Lights=OFF"); sensorState=getSensors (type="ALL|SensorName|SensorNameList"); result=setSensorState(SensorName, parameters="Option**1**, Options**2**, . . . Option n"); interrupthandler=SensorEvent( ); and, interruptHandler=alarmEvent( ).

Functions of the remote service APIs **1212** of an embodiment use a remote PanelConnect API **1224** which resides in memory on the gateway **1202**. The touchscreen **1203** communicates with the gateway **1202** through a suitable network interface such as an Ethernet or 802.11 RF connection, for example. The remote PanelConnect API **1224** provides the underlying Security System Interfaces **1226** used to communicate with and control one or more types of security panel via wired link **1230** and/or RF link **3**. The PanelConnect API **1224** provides responses and input to the remote services APIs **1226**, and in turn translates function calls and data to and from the specific protocols and functions supported by a specific implementation of a Security Panel (e.g. a GE Security Simon XT or Honeywell Vista 20P). In an embodiment, the PanelConnect API **1224** uses a 345 MHz RF transceiver or receiver hardware/firmware module to communicate wirelessly to the security panel and directly to a set of 345 MHz RF-enabled sensors and devices, but the embodiment is not so limited.

The gateway of an alternative embodiment communicates over a wired physical coupling or connection to the security panel using the panel's specific wired hardware (bus) interface and the panel's bus-level protocol.

In an alternative embodiment, the Touchscreen **1203** implements the same PanelConnect API **1214** locally on the Touchscreen **1203**, communicating directly with the Security Panel **2** and/or Sensors **2** over the proprietary RF link or over a wired link for that system. In this embodiment the Touchscreen **1203**, instead of the gateway **1202**, incorporates the 345 MHz RF transceiver to communicate directly with Security Panel **2** or Sensors **2** over the RF link **2**. In the case of a wired link the Touchscreen **1203** incorporates the real-time hardware (e.g. a PIC chip and RS232-variant serial link) to physically connect to and satisfy the specific bus-level timing requirements of the SecurityPanel2.

In yet another alternative embodiment, either the gateway **1202** or the Touchscreen **1203** implements the remote service APIs. This embodiment includes a Cricket device ("Cricket") which comprises but is not limited to the following components: a processor (suitable for handling 802.11 protocols and processing, as well as the bus timing requirements of SecurityPanel**1**); an 802.11 (WiFi) client IP interface chip; and, a serial bus interface chip that implements variants of RS232 or RS485, depending on the specific Security Panel.

The Cricket also implements the full PanelConnect APIs such that it can perform the same functions as the case where the gateway implements the PanelConnect APIs. In this embodiment, the touchscreen core application **1210** calls functions in the remote service APIs **1212** (such as setArmState( )). These functions in turn couple or connect to the remote Cricket through a standard IP connection ("Cricket IP Link") (e.g., Ethernet, Homeplug, the gateway's proprietary Wifi network, etc.). The Cricket in turn implements the PanelConnect API, which responds to the request from the touchscreen core application, and performs the appropriate function using the proprietary panel interface. This interface uses either the wireless or wired proprietary protocol for the specific security panel and/or sensors.

An example use case that illustrates the use of the touchscreen embodiments described above is a panic alarm. FIG. **13** is a data flow diagram for a panic alarm **1300**, under an embodiment. In order to activate a panic alarm on the touchscreen, the user presses one of the panic alarm buttons, and confirms the alarm with a second button press (Step **1**). When the alarm is activated, in Step **2** the touchscreen sends the alarm signal to both the security panel and the gateway (using the PanelConnect or remote Svc API interface described above).

In Step **3**, the security panel alerts other keypads and touchscreens (once again through the PanelConnect interface) of the alarm condition, and flashes lights/sounds sirens as appropriate. The gateway or security panel calls the CMS on the hard-wired phone line. Simultaneously, the gateway sends a signal to the iConnect Server system over the broadband connection and, if so configured, uses GPRS to call a cell phone relay station with the alarm data. In Step **4**, the iConnect Server system routes the information, formatted using an industry standard alarm format such as ContactID or SIA, to a suitable broadband receiver in the CMS (for example the DSC Surguard broadband alarm receiver, or directly to the CMS automation software server). At the same time, in Step

5 the server system will also call a phone, send an SMS message, or send an email to any designated receiver.

The second example use case involving the touchscreen is a device installation example. FIG. **14** is a data flow diagram for device installation **1400**, under an embodiment. To make installation easier, the user can receive feedback from the touchscreen about what devices have been programmed in to the system, and the system automatically couples or connects to the CMS to configure the sensors on the back end.

As a data flow, in Step **1** the installer initiates entry into sensor learning mode by activating the installation UI on the touchscreen. When the installer triggers or otherwise activates a sensor in Step **2**, the gateway picks up the wireless communication from the sensor and pushes information about the sensor to the touchscreen (Step **3**). At this point, the installer can program the specific name of the sensor and its zones. This process is repeated for all of the sensors in the system. Once all sensors have been 'learned' in this way, the information is transmitted via internet or cellular IP networks to the iConnect server. The sensor information is associated with a 'network' (e.g., a location), but has not yet been associated with a specific user or account. After this step, the installer then creates a user account, and the previously created network is then associated with that account in the iConnect user database. This embodiment allows systems, devices, touchscreens, panels, and the like to be pre-associated, packaged, and/or installed without reference to a user or subscriber account.

To ensure that the security system is operating properly, it is next put into test mode. As the installer opens and closes the sensor, the touchscreen places a 'check' next to the name of the sensor. At the same time, in Step **4** the gateway pushes the open/close information to the iConnect servers, which alert the CMS to verify that a signal has been received for the sensor on the back end. In Step **5**, the CMS acknowledges that the sensor has been installed correctly and is operational, and that acknowledgement is pushed back through the system. When the system installation is finished, the iConnect servers send a notification of the installation, along with sensor set up information, and electronic verification of the test process for all sensors to the service provider.

Yet another example use case involving the touchscreen is a camera event. FIG. **15** is a data flow diagram for a camera event **1500**, under an embodiment. Cameras can be integrated with alerts that are generated by sensor events. For example, a consumer who wishes to see who is at her front door would set up the front door sensor to trigger an iControl Notification to the touchscreen, signifying a camera alert. When the sensor is activated, a pop-up appears on the touchscreen telling the user that the front door sensor has been activated, and asking the user if he or she would like to view the video.

The flow diagram for the camera event **1500** shows the flow of data from the sensor to the security panel and the gateway during a camera event. The gateway receives information regarding automation 'rules' between camera and sensor event from the iConnect servers as a part of the periodic state updates that occur between gateway client and server.

In Step **1** a sensor or multiple sensors are triggered. In Step **2** the gateway and/or Security Panel receives notification that a sensor state has changed through a network connection (wired or wireless) with the sensor, and if a rule exists for that device or set of devices, the touchscreen is then alerted via the PanelConnect interface running either locally on the touchscreen or remotely on the gateway. In Step **3**, the touchscreen puts up the alert and, if requested, opens a video stream from the camera. In the event that the touchscreen is in a quiescent mode instead of a dialog popup the IP video is immediately displayed, and an audible alert may sound as an option in the notification.

Step **3** of the data flow also shows an alternate route over which the gateway, if so configured, can send the sensor information the iControl servers (Step **4**), which in turn forward the information in the form of an SMS alert or direct IP notification to a cell phone (Step **5**). The cell phone user could then set up a video stream from the camera.

FIG. **16** is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment. Operations begin when the system is powered on **1610**, involving at a minimum the power-on of the gateway device, and optionally the power-on of the connection between the gateway device and the remote servers. The gateway device initiates **1620** a software and RF sequence to locate the extant security system. The gateway and installer initiate and complete **1630** a sequence to 'learn' the gateway into the security system as a valid and authorized control device. The gateway initiates **1640** another software and RF sequence of instructions to discover and learn the existence and capabilities of existing RF devices within the extant security system, and store this information in the system. These operations under the system of an embodiment are described in further detail below.

Unlike conventional systems that extend an existing security system, the system of an embodiment operates utilizing the proprietary wireless protocols of the security system manufacturer. In one illustrative embodiment, the gateway is an embedded computer with an IP LAN and WAN connection and a plurality of RF transceivers and software protocol modules capable of communicating with a plurality of security systems each with a potentially different RF and software protocol interface. After the gateway has completed the discovery and learning **1640** of sensors and has been integrated **1650** as a virtual control device in the extant security system, the system becomes operational. Thus, the security system and associated sensors are presented **1650** as accessible devices to a potential plurality of user interface subsystems.

The system of an embodiment integrates **1660** the functionality of the extant security system with other non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms, which may be controlled via RF, wired, or powerline-based networking mechanisms supported by the gateway or servers.

The system of an embodiment provides a user interface subsystem **1670** enabling a user to monitor, manage, and control the system and associated sensors and security systems. In an embodiment of the system, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX/Flash presentation of a monitoring and control application, enabling users to view the state of all sensors and controllers in the extant security system from a web browser or equivalent operating on a computer, PDA, mobile phone, or other consumer device.

In another illustrative embodiment of the system described herein, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX presentation of a monitoring and control application, enabling users to combine the monitoring and control of the extant security system and sensors with the monitoring and control of non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms.

In another illustrative embodiment of the system described herein, a user interface subsystem is a mobile phone application enabling users to monitor and control the extant security system as well as other non-security devices.

In another illustrative embodiment of the system described herein, a user interface subsystem is an application running on a keypad or touchscreen device enabling users to monitor and control the extant security system as well as other non-security devices.

In another illustrative embodiment of the system described herein, a user interface subsystem is an application operating on a TV or set-top box connected to a TV enabling users to monitor and control the extant security system as well as other non-security devices.

FIG. **17** is a block diagram of an integrated security system **1700** wirelessly interfacing to proprietary security systems, under an embodiment. A security system **1710** is coupled or connected to a Gateway **1720**, and from Gateway **1720** coupled or connected to a plurality of information and content sources across a network **1730** including one or more web servers **1740**, system databases **1750**, and applications servers **1760**. While in one embodiment network **1730** is the Internet, including the World Wide Web, those of skill in the art will appreciate that network **1730** may be any type of network, such as an intranet, an extranet, a virtual private network (VPN), a mobile network, or a non-TCP/IP based network.

Moreover, other elements of the system of an embodiment may be conventional, well-known elements that need not be explained in detail herein. For example, security system **1710** could be any type home or business security system, such devices including but not limited to a standalone RF home security system or a non-RF-capable wired home security system with an add-on RF interface module. In the integrated security system **1700** of this example, security system **1710** includes an RF-capable wireless security panel (WSP) **1711** that acts as the master controller for security system **1710**. Well-known examples of such a WSP include the GE Security Concord, Network, and Simon panels, the Honeywell Vista and Lynx panels, and similar panels from DSC and Napco, to name a few. A wireless module **1714** includes the RF hardware and protocol software necessary to enable communication with and control of a plurality of wireless devices **1713**. WSP **1711** may also manage wired devices **1714** physically connected to WSP **1711** with an RS232 or RS485 or Ethernet connection or similar such wired interface.

In an implementation consistent with the systems and methods described herein, Gateway **1720** provides the interface between security system **1710** and LAN and/or WAN for purposes of remote control, monitoring, and management. Gateway **1720** communicates with an external web server **1740**, database **1750**, and application server **1760** over network **1730** (which may comprise WAN, LAN, or a combination thereof). In this example system, application logic, remote user interface functionality, as well as user state and account are managed by the combination of these remote servers. Gateway **1720** includes server connection manager **1721**, a software interface module responsible for all server communication over network **1730**. Event manager **1722** implements the main event loop for Gateway **1720**, processing events received from device manager **1724** (communicating with non-security system devices including but not limited to IP cameras, wireless thermostats, or remote door locks). Event manager **1722** further processes events and control messages from and to security system **1710** by utilizing WSP manager **1723**.

WSP manager **1723** and device manager **1724** both rely upon wireless protocol manager **1726** which receives and stores the proprietary or standards-based protocols required to support security system **1710** as well as any other devices interfacing with gateway **1720**. WSP manager **1723** further utilizes the comprehensive protocols and interface algorithms for a plurality of security systems **1710** stored in the WSP DB client database associated with wireless protocol manager **1726**. These various components implement the software logic and protocols necessary to communicate with and manager devices and security systems **1710**. Wireless Transceiver hardware modules **1725** are then used to implement the physical RF communications link to such devices and security systems **1710**. An illustrative wireless transceiver **1725** is the GE Security Dialog circuit board, implementing a 319.5 MHz two-way RF transceiver module. In this example, RF Link **1770** represents the 319.5 MHz RF communication link, enabling gateway **1720** to monitor and control WSP **1711** and associated wireless and wired devices **1713** and **1714**, respectively.

In one embodiment, server connection manager **1721** requests and receives a set of wireless protocols for a specific security system **1710** (an illustrative example being that of the GE Security Concord panel and sensors) and stores them in the WSP DB portion of the wireless protocol manager **1726**. WSP manager **1723** then utilizes such protocols from wireless protocol manager **1726** to initiate the sequence of processes detailed in FIG. **16** and FIG. **17** for learning gateway **1720** into security system **1710** as an authorized control device. Once learned in, as described with reference to FIG. **17** (and above), event manager **1722** processes all events and messages detected by the combination of WSP manager **1723** and the GE Security wireless transceiver module **1725**.

In another embodiment, gateway **1720** incorporates a plurality of wireless transceivers **1725** and associated protocols managed by wireless protocol manager **1726**. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP **1711**, wireless devices **1713**, and wired devices **1714**. For example a wireless sensor from one manufacturer may be utilized to control a device using a different protocol from a different manufacturer.

In another embodiment, gateway **1720** incorporates a wired interface to security system **1710**, and incorporates a plurality of wireless transceivers **1725** and associated protocols managed by wireless protocol manager **1726**. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP **1711**, wireless devices **1713**, and wired devices **1714**.

Of course, while an illustrative embodiment of an architecture of the system of an embodiment is described in detail herein with respect to FIG. **17**, one of skill in the art will understand that modifications to this architecture may be made without departing from the scope of the description presented herein. For example, the functionality described herein may be allocated differently between client and server, or amongst different server or processor-based components. Likewise, the entire functionality of the gateway **1720** described herein could be integrated completely within an existing security system **1710**. In such an embodiment, the architecture could be directly integrated with a security system **1710** in a manner consistent with the currently described embodiments.

FIG. **18** is a flow diagram for wirelessly 'learning' the Gateway into an existing security system and discovering extant sensors, under an embodiment. The learning interfaces gateway **1720** with security system **1710**. Gateway **1720** powers up **1810** and initiates software sequences **1820** and **1825** to identify accessible WSPs **1711** and wireless devices **1713**, respectively (e.g., one or more WSPs and/or devices within range of gateway **1720**). Once identified, WSP **1711** is manually or automatically set into 'learn mode' **1830**, and gateway **1720** utilizes available protocols to add **1840** itself as an authorized control device in security system **1710**. Upon successful completion of this task, WSP **1711** is manually or automatically removed from 'learn mode' **1850**.

Gateway **1720** utilizes the appropriate protocols to mimic **1860** the first identified device **1714**. In this operation gateway **1720** identifies itself using the unique or pseudo-unique identifier of the first found device **1714**, and sends an appropriate change of state message over RF Link **1770**. In the event that WSP **1711** responds to this change of state message, the device **1714** is then added **1870** to the system in database **1750**. Gateway **1720** associates **1880** any other information (such as zone name or token-based identifier) with this device **1714** in database **1750**, enabling gateway **1720**, user interface modules, or any application to retrieve this associated information.

In the event that WSP **1711** does not respond to the change of state message, the device **1714** is not added **1870** to the system in database **1750**, and this device **1714** is identified as not being a part of security system **1710** with a flag, and is either ignored or added as an independent device, at the discretion of the system provisioning rules. Operations hereunder repeat **1885** operations **1860**, **1870**, **1880** for all devices **1714** if applicable. Once all devices **1714** have been tested in this way, the system begins operation **1890**.

In another embodiment, gateway **1720** utilizes a wired connection to WSP **1711**, but also incorporates a wireless transceiver **1725** to communicate directly with devices **1714**. In this embodiment, operations under **1820** above are removed, and operations under **1840** above are modified so the system of this embodiment utilizes wireline protocols to add itself as an authorized control device in security system **1710**.

A description of an example embodiment follows in which the Gateway (FIG. **17**, element **1720**) is the iHub available from iControl Networks, Palo Alto, Calif., and described in detail herein. In this example the gateway is "automatically" installed with a security system.

The automatic security system installation begins with the assignment of an authorization key to components of the security system (e.g., gateway, kit including the gateway, etc.). The assignment of an authorization key is done in lieu of creating a user account. An installer later places the gateway in a user's premises along with the premises security system. The installer uses a computer to navigate to a web portal (e.g., integrated security system web interface), logs in to the portal, and enters the authorization key of the installed gateway into the web portal for authentication. Once authenticated, the gateway automatically discovers devices at the premises (e.g., sensors, cameras, light controls, etc.) and adds the discovered devices to the system or "network". The installer assigns names to the devices, and tests operation of the devices back to the server (e.g., did the door open, did the camera take a picture, etc.). The security device information is optionally pushed or otherwise propagated to a security panel and/or to the server network database. The installer finishes the installation, and instructs the end user on how to create an account, username, and password. At this time the user enters the authorization key which validates the account creation (uses a valid authorization key to associate the network with the user's account). New devices may subsequently be added to the security network in a variety of ways (e.g., user first enters a unique ID for each device/sensor and names it in the server, after which the gateway can automatically discover and configure the device).

A description of another example embodiment follows in which the security system (FIG. **17**, element **1710**) is a Dialog system and the WSP (FIG. **17**, element **1711**) is a SimonXT available from General Electric Security, and the Gateway (FIG. **17**, element **1720**) is the iHub available from iControl Networks, Palo Alto, Calif., and described in detail herein. Descriptions of the install process for the SimonXT and iHub are also provided below.

GE Security's Dialog network is one of the most widely deployed and tested wireless security systems in the world. The physical RF network is based on a 319.5 MHz unlicensed spectrum, with a bandwidth supporting up to 19 Kbps communications. Typical use of this bandwidth even in conjunction with the integrated security system—is far less than that. Devices on this network can support either one-way communication (either a transmitter or a receiver) or two-way communication (a transceiver). Certain GE Simon, Simon XT, and Concord security control panels incorporate a two-way transceiver as a standard component. The gateway also incorporates the same two-way transceiver card. The physical link layer of the network is managed by the transceiver module hardware and firmware, while the coded payload bitstreams are made available to the application layer for processing.

Sensors in the Dialog network typically use a 60-bit protocol for communicating with the security panel transceiver, while security system keypads and the gateway use the encrypted 80-bit protocol. The Dialog network is configured for reliability, as well as low-power usage. Many devices are supervised, i.e. they are regularly monitored by the system 'master' (typically a GE security panel), while still maintaining excellent power usage characteristics. A typical door window sensor has a battery life in excess of 5-7 years.

The gateway has two modes of operation in the Dialog network: a first mode of operation is when the gateway is configured or operates as a 'slave' to the GE security panel; a second mode of operation is when the gateway is configured or operates as a 'master' to the system in the event a security panel is not present. In both configurations, the gateway has the ability to 'listen' to network traffic, enabling the gateway to continually keep track of the status of all devices in the system. Similarly, in both situations the gateway can address and control devices that support setting adjustments (such as the GE wireless thermostat).

In the configuration in which the gateway acts as a 'slave' to the security panel, the gateway is 'learned into' the system as a GE wireless keypad. In this mode of operation, the gateway emulates a security system keypad when managing the security panel, and can query the security panel for status and 'listen' to security panel events (such as alarm events).

The gateway incorporates an RF Transceiver manufactured by GE Security, but is not so limited. This transceiver implements the Dialog protocols and handles all network message transmissions, receptions, and timing. As such, the physical, link, and protocol layers of the communications between the gateway and any GE device in the Dialog network are totally compliant with GE Security specifications.

At the application level, the gateway emulates the behavior of a GE wireless keypad utilizing the GE Security 80-bit encrypted protocol, and only supported protocols and network traffic are generated by the gateway. Extensions to the Dialog RF protocol of an embodiment enable full control and configuration of the panel, and iControl can both automate installation and sensor enrollment as well as direct configuration downloads for the panel under these protocol extensions.

As described above, the gateway participates in the GE Security network at the customer premises. Because the gateway has intelligence and a two-way transceiver, it can 'hear' all of the traffic on that network. The gateway makes use of the periodic sensor updates, state changes, and supervisory signals of the network to maintain a current state of the premises. This data is relayed to the integrated security system server (e.g., FIG. **2**, element **260**) and stored in the event repository for use by other server components. This usage of the GE Security RF network is completely non-invasive; there is no new data traffic created to support this activity.

The gateway can directly (or indirectly through the Simon XT panel) control two-way devices on the network. For example, the gateway can direct a GE Security Thermostat to change its setting to 'Cool' from 'Off', as well as request an update on the current temperature of the room. The gateway performs these functions using the existing GE Dialog protocols, with little to no impact on the network; a gateway device control or data request takes only a few dozen bytes of data in a network that can support 19 Kbps.

By enrolling with the Simon XT as a wireless keypad, as described herein, the gateway includes data or information of all alarm events, as well as state changes relevant to the security panel. This information is transferred to the gateway as encrypted packets in the same way that the information is transferred to all other wireless keypads on the network.

Because of its status as an authorized keypad, the gateway can also initiate the same panel commands that a keypad can initiate. For example, the gateway can arm or disarm the panel using the standard Dialog protocol for this activity. Other than the monitoring of standard alarm events like other network keypads, the only incremental data traffic on the network as a result of the gateway is the infrequent remote arm/disarm events that the gateway initiates, or infrequent queries on the state of the panel.

The gateway is enrolled into the Simon XT panel as a 'slave' device which, in an embodiment, is a wireless keypad. This enables the gateway for all necessary functionality for operating the Simon XT system remotely, as well as combining the actions and information of non-security devices such as lighting or door locks with GE Security devices. The only resource taken up by the gateway in this scenario is one wireless zone (sensor ID).

The gateway of an embodiment supports three forms of sensor and panel enrollment/installation into the integrated security system, but is not limited to this number of enrollment/installation options. The enrollment/installation options of an embodiment include installer installation, kitting, and panel, each of which is described below.

Under the installer option, the installer enters the sensor IDs at time of installation into the integrated security system web portal or iScreen. This technique is supported in all configurations and installations.

Kits can be pre-provisioned using integrated security system provisioning applications when using the kitting option. At kitting time, multiple sensors are automatically associated with an account, and at install time there is no additional work required.

In the case where a panel is installed with sensors already enrolled (i.e. using the GE Simon XT enrollment process), the gateway has the capability to automatically extract the sensor information from the system and incorporate it into the user account on the integrated security system server.

The gateway and integrated security system of an embodiment uses an auto-learn process for sensor and panel enrollment in an embodiment. The deployment approach of an embodiment can use additional interfaces that GE Security is adding to the Simon XT panel. With these interfaces, the gateway has the capability to remotely enroll sensors in the panel automatically. The interfaces include, but are not limited to, the following: EnrollDevice(ID, type, name, zone, group); SetDeviceParameters(ID, type, Name, zone, group), GetDeviceParameters(zone); and RemoveDevice(zone).

The integrated security system incorporates these new interfaces into the system, providing the following install process. The install process can include integrated security system logistics to handle kitting and pre-provisioning. Pre-kitting and logistics can include a pre-provisioning kitting tool provided by integrated security system that enables a security system vendor or provider ("provider") to offer pre-packaged initial 'kits'. This is not required but is recommended for simplifying the install process. This example assumes a 'Basic' kit is preassembled and includes one (1) Simon XT, three (3) Door/window sensors, one (1) motion sensor, one (1) gateway, one (1) keyfob, two (2) cameras, and ethernet cables. The kit also includes a sticker page with all Zones (1-24) and Names (full name list).

The provider uses the integrated security system kitting tool to assemble 'Basic' kit packages. The contents of different types of starter kits may be defined by the provider. At the distribution warehouse, a worker uses a bar code scanner to scan each sensor and the gateway as it is packed into the box. An ID label is created that is attached to the box. The scanning process automatically associates all the devices with one kit, and the new ID label is the unique identifier of the kit. These boxes are then sent to the provider for distribution to installer warehouses. Individual sensors, cameras, etc. are also sent to the provider installer warehouse. Each is labeled with its own barcode/ID.

An installation and enrollment procedure of a security system including a gateway is described below as one example of the installation process.

1. Order and Physical Install Process
   a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the provider for assignment to an installer.
   b. The assigned installer picks up his/her ticket(s) and fills his/her truck with Basic and/or Advanced starter kits. He/she also keeps a stock of individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.
   c. The installer arrives at the address on the ticket, and pulls out the Basic kit. The installer determines sensor locations from a tour of the premises and discussion with the homeowner. At this point assume the homeowner requests additional equipment including an extra camera, two (2) additional door/window sensors, one (1) glass break detector, and one (1) smoke detector.
   d. Installer mounts SimonXT in the kitchen or other location in the home as directed by the homeowner, and routes the phone line to Simon XT if available. GPRS and Phone numbers pre-programmed in SimonXT to point to the provider Central Monitoring Station (CMS).
   e. Installer places gateway in the home in the vicinity of a router and cable modem. Installer installs an ethernet line from gateway to router and plugs gateway into an electrical outlet.
2. Associate and Enroll gateway into SimonXT
   a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with installer ID/pass.
   b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer for kit ID (on box's barcode label).
   c. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add

gateway as a wireless keypad. It is noted that this step is for security only and can be automated in an embodiment.

d. Installer enters the installer code into the Simon XT. Installer Learns 'gateway' into the panel as a wireless keypad as a group 1 device.

e. Installer goes back to Web portal, and clicks the 'Finished Adding SimonXT' button.

3. Enroll Sensors into SimonXT via iControl

a. All devices in the Basic kit are already associated with the user's account.

b. For additional devices, Installer clicks 'Add Device' and adds the additional camera to the user's account (by typing in the camera ID/Serial #).

c. Installer clicks 'Add Device' and adds other sensors (two (2) door/window sensors, one (1) glass break sensor, and one (1) smoke sensor) to the account (e.g., by typing in IDs).

d. As part of Add Device, Installer assigns zone, name, and group to the sensor. Installer puts appropriate Zone and Name sticker on the sensor temporarily.

e. All sensor information for the account is pushed or otherwise propagated to the iConnect server, and is available to propagate to CMS automation software through the CMS application programming interface (API).

f. Web interface displays 'Installing Sensors in System . . . ' and automatically adds all of the sensors to the Simon XT panel through the GE RF link.

g. Web interface displays 'Done Installing'-->all sensors show green.

4. Place and Tests Sensors in Home

a. Installer physically mounts each sensor in its desired location, and removes the stickers.

b. Installer physically mounts WiFi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.

c. Installer goes to Web interface and is prompted for automatic camera install. Each camera is provisioned as a private, encrypted Wifi device on the gateway secured sandbox network, and firewall NAT traversal is initiated. Upon completion the customer is prompted to test the security system.

d. Installer selects the 'Test System' button on the web portal—the SimonXT is put into Test mode by the gateway over GE RF.

e. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.

f. gateway sends test data directly to CMS over broadband link, as well as storing the test data in the user's account for subsequent report generation.

g. Installer exits test mode from the Web portal.

5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the iControl web and mobile portals. Customer creates a username/password at this time.

6. Installer instructs customer how to change Simon XT user code from the Web interface. Customer changes user code which is pushed to SimonXT automatically over GE RF.

An installation and enrollment procedure of a security system including a gateway is described below as an alternative example of the installation process. This installation process is for use for enrolling sensors into the SimonXT and integrated security system and is compatible with all existing GE Simon panels.

The integrated security system supports all pre-kitting functionality described in the installation process above. However, for the purpose of the following example, no kitting is used.

1. Order and Physical Install Process

a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the security system provider for assignment to an installer.

b. The assigned installer picks up his/her ticket(s) and fills his/her truck with individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.

c. The installer arrives at the address on the ticket, and analyzes the house and talks with the homeowner to determine sensor locations. At this point assume the homeowner requests three (3) cameras, five (5) door/window sensors, one (1) glass break detector, one (1) smoke detector, and one (1) keyfob.

d. Installer mounts SimonXT in the kitchen or other location in the home. The installer routes a phone line to Simon XT if available. GPRS and Phone numbers are pre-programmed in SimonXT to point to the provider CMS.

e. Installer places gateway in home in the vicinity of a router and cable modem, and installs an ethernet line from gateway to the router, and plugs gateway into an electrical outlet.

2. Associate and Enroll gateway into SimonXT

a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with an installer ID/pass.

b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer to add devices.

c. Installer types in ID of gateway, and it is associated with the user's account.

d. Installer clicks 'Add Device' and adds the cameras to the user's account (by typing in the camera ID/Serial #).

e. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add gateway as a wireless keypad.

f. Installer goes to Simon XT and enters the installer code into the Simon XT. Learns 'gateway' into the panel as a wireless keypad as group 1 type sensor.

g. Installer returns to Web portal, and clicks the 'Finished Adding SimonXT' button.

h. Gateway now is alerted to all subsequent installs over the security system RF.

3. Enroll Sensors into SimonXT via iControl

a. Installer clicks 'Add Simon XT Sensors'—Displays instructions for adding sensors to Simon XT.

b. Installer goes to Simon XT and uses Simon XT install process to add each sensor, assigning zone, name, group. These assignments are recorded for later use.

c. The gateway automatically detects each sensor addition and adds the new sensor to the integrated security system.

d. Installer exits install mode on the Simon XT, and returns to the Web portal.

e. Installer clicks 'Done Adding Devices'.

f. Installer enters zone/sensor naming from recorded notes into integrated security system to associate sensors to friendly names.

g. All sensor information for the account is pushed to the iConnect server, and is available to propagate to CMS automation software through the CMS API.

4. Place and Tests Sensors in Home
   a. Installer physically mounts each sensor in its desired location.
   b. Installer physically mounts Wifi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
   c. Installer puts SimonXT into Test mode from the keypad.
   d. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
   e. Installer exits test mode from the Simon XT keypad.
   f. Installer returns to web interface and is prompted to automatically set up cameras. After waiting for completion cameras are now provisioned and operational.
5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the integrated security system web and mobile portals. Customer creates a username/password at this time.
6. Customer and Installer observe that all sensors/cameras are green.
7. Installer instructs customer how to change Simon XT user code from the keypad. Customer changes user code and stores in SimonXT.
8. The first time the customer uses the web portal to Arm/Disarm system the web interface prompts the customer for the user code, which is then stored securely on the server. In the event the user code is changed on the panel the web interface once again prompts the customer.

The panel of an embodiment can be programmed remotely. The CMS pushes new programming to SimonXT over a telephone or GPRS link. Optionally, iControl and GE provide a broadband link or coupling to the gateway and then a link from the gateway to the Simon XT over GE RF.

As described above, computer networks suitable for use with the embodiments described herein include local area networks (LAN), wide area networks (WAN), Internet, or other connection services and network variations such as the world wide web, the public internet, a private internet, a private computer network, a public network, a mobile network, a cellular network, a value-added network, and the like. Computing devices coupled or connected to the network may be any microprocessor controlled device that permits access to the network, including terminal devices, such as personal computers, workstations, servers, mini computers, mainframe computers, laptop computers, mobile computers, palm top computers, hand held computers, mobile phones, TV set-top boxes, or combinations thereof. The computer network may include one of more LANs, WANs, Internets, and computers. The computers may serve as servers, clients, or a combination thereof.

The integrated security system can be a component of a single system, multiple systems, and/or geographically separate systems. The integrated security system can also be a subcomponent or subsystem of a single system, multiple systems, and/or geographically separate systems. The integrated security system can be coupled to one or more other components (not shown) of a host system or a system coupled to the host system.

One or more components of the integrated security system and/or a corresponding system or application to which the integrated security system is coupled or connected includes and/or runs under and/or in association with a processing system. The processing system includes any collection of processor-based devices or computing devices operating together, or components of processing systems or devices, as is known in the art. For example, the processing system can include one or more of a portable computer, portable communication device operating in a communication network, and/or a network server. The portable computer can be any of a number and/or combination of devices selected from among personal computers, personal digital assistants, portable computing devices, and portable communication devices, but is not so limited. The processing system can include components within a larger computer system.

The processing system of an embodiment includes at least one processor and at least one memory device or subsystem. The processing system can also include or be coupled to at least one database. The term "processor" as generally used herein refers to any logic processing unit, such as one or more central processing units (CPUs), digital signal processors (DSPs), application-specific integrated circuits (ASIC), etc. The processor and memory can be monolithically integrated onto a single chip, distributed among a number of chips or components, and/or provided by some combination of algorithms. The methods described herein can be implemented in one or more of software algorithm(s), programs, firmware, hardware, components, circuitry, in any combination.

The components of any system that includes the integrated security system can be located together or in separate locations. Communication paths couple the components and include any medium for communicating or transferring files among the components. The communication paths include wireless connections, wired connections, and hybrid wireless/wired connections. The communication paths also include couplings or connections to networks including local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), proprietary networks, interoffice or backend networks, and the Internet. Furthermore, the communication paths include removable fixed mediums like floppy disks, hard disk drives, and CD-ROM disks, as well as flash RAM, Universal Serial Bus (USB) connections, RS-232 connections, telephone lines, buses, and electronic mail messages.

Embodiments of the integrated security system include a device comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; and a plurality of interfaces coupled to the processor and presented to a user via the touchscreen, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a wide area network (WAN) coupled to the LAN; and a remote server coupled to the touchscreen, the remote server managing at least one of the touchscreen and the security system.

The remote server of an embodiment allows a user to configure content of the touchscreen.

The remote server of an embodiment provides user portals that enable content and information displayed on the touchscreen to be displayed on other devices.

The other devices of an embodiment include at least one of HTML browsers, WEB/WAP phones, and desktop widgets.

The security system of an embodiment is managed via applications entirely within the touchscreen.

The touchscreen of an embodiment includes a wireless transceiver for communicating with security system components of the security system.

The touchscreen of an embodiment plays live video from a camera, wherein the camera is an Internet Protocol (IP) camera.

The camera of an embodiment is at the first location.

The camera of an embodiment is at a second location managed by the remote server.

The live video of an embodiment is accessed through internet content widgets.

The live video of an embodiment is IP video.

The live video of an embodiment is MPEG-4 video.

The live video of an embodiment is Motion JPEG (MJPEG) video.

Devices of an embodiment are added to the security system through the touchscreen.

Devices of an embodiment are added to a user account on the remote server through the touchscreen.

Device information and device data of an embodiment are transmitted to from the devices to the remote server.

The device information of an embodiment includes at least one of device name and device type, wherein the device data includes at least one of device state and battery state.

Device information and device data of an embodiment are associated with a user account by the remote server.

The devices of an embodiment are automatically detected by the touchscreen and added to a user account on the remote server through the touchscreen.

The coupling with the LAN of an embodiment is over 802.11.

The touchscreen of an embodiment integrates the content with the access and control of the security system.

The content of an embodiment includes interactive content in the form of internet widgets.

The network interface of an embodiment allows the user to transfer at least one of content and internet widgets to and from the LAN.

The network interface of an embodiment allows the user to control functions of peripheral devices of the first location coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides the user with communication and control of a plurality of network devices coupled to the LAN.

The network interface of an embodiment provides the user with communication and control of a plurality of security system components, wherein the security system comprises the plurality of security system components.

The WAN of an embodiment is the internet and the network interface of an embodiment is a web browser.

The touchscreen of an embodiment integrates at least one of a security system control panel and an internet browser.

The device of an embodiment comprises an application engine coupled to the processor, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

The plurality of devices of an embodiment are coupled to the processor.

The plurality of devices of an embodiment are coupled to the processor via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the WAN.

The plurality of applications of an embodiment are accessed and loaded directly via the WAN.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between the plurality of devices.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The device of an embodiment comprises a first application engine coupled to the processor, wherein the first application engine executes a security application that provides the security interface. The device of an embodiment comprises a second application engine coupled to the processor, wherein the second application engine executes a content application that provides the network interface.

The device of an embodiment comprises a core engine coupled to the processor, the core engine controlling dynamic provisioning of the plurality of applications and the content.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The processor of an embodiment is coupled to the WAN via a broadband coupling.

The processor of an embodiment is coupled to the WAN via a cellular data coupling.

The plurality of interfaces of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

The device controller of an embodiment is a thermostat.

The device controller of an embodiment is an energy meter.

A device of the plurality of devices of an embodiment is a sensor.

The network interface of an embodiment allows a user to control functions of peripheral devices coupled to other touchscreens located at remote locations.

Embodiments of the integrated security system include a device comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; a plurality of applications coupled to the processor, the plurality of applications displaying a plurality of interfaces to a user via the touchscreen, the plurality of interfaces including a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN; and a remote server coupled to the touchscreen, the remote server managing at least one of the touchscreen and the security system.

Embodiments of the integrated security system include a device comprising: an input/output (I/O) device at a first location, the I/O device comprising a processor coupled to a local area network (LAN) and a security system at the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system; a security application coupled to the processor, the security application providing a security interface for control of functions of the security system, the security interface presented to a user via the I/O device; a content application coupled to a processor, the content application providing a network interface for access to networked content of a remote wide area network (WAN), the network interface presented to a user via the I/O device, wherein the I/O device is coupled to the WAN via the LAN; and a remote server coupled to the I/O device, the remote server managing at least one of the I/O device and the security system.

Embodiments of the integrated security system include a system comprising: a gateway at a first location, the gateway coupled to a local area network (LAN) and a security system of the first location, wherein the security system includes a plurality of security system components, the gateway forming a security network that integrates functions of the security system with the LAN; a touchscreen coupled to the gateway, the touchscreen including a plurality of interfaces presented to a user, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides interactivity with the security system, wherein the network interface provides interactivity with networked content of a remote network.

The system of an embodiment comprises a security server located at a second location different from the first location, the security server coupled to the gateway, the touchscreen providing interactivity with networked content of a remote network via the security server.

The security interface of an embodiment provides the user with control of functions of the security system and access to data collected by the security system

The network interface of an embodiment allows the user to transfer content to and from a wide area network (WAN) coupled to the LAN.

The gateway of an embodiment integrates the content with access and control of the security system.

The content of an embodiment includes interactive content.

The network interface of an embodiment allows the user to transfer content to and from the LAN.

The network interface of an embodiment allows the user to control functions of network devices of the first location coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides interactivity with a plurality of network devices coupled to the LAN.

The security interface of an embodiment provides the user with communication and control of the plurality of security system components.

The remote network of an embodiment is the internet and the network interface is a web browser.

The touchscreen of an embodiment integrates a security system control panel and an internet browser.

The system of an embodiment comprises an application engine coupled to the touchscreen, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

The plurality of devices of an embodiment are coupled to at least one of the touchscreen and the gateway.

The plurality of devices of an embodiment are coupled to at least one of the touchscreen and the gateway via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the remote network.

The plurality of applications of an embodiment are accessed and loaded directly via the remote network.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between a plurality of devices comprising at least one of the security system components, network devices coupled to the LAN, and devices coupled to the remote network.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The system of an embodiment comprises a first application engine coupled to the touchscreen, wherein the first application engine executes a security application that provides the security interface. The system of an embodiment comprises a second application engine coupled to the touchscreen, wherein the second application engine executes a content application that provides the network interface.

The system of an embodiment comprises a core engine coupled to the touchscreen, the core engine controlling dynamic provisioning of a plurality of applications and the content, the plurality of applications corresponding to the plurality of interfaces.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The touchscreen of an embodiment is coupled to the remote network via a broadband coupling.

The touchscreen of an embodiment is coupled to the remote network via a cellular coupling.

A plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

A device of the plurality of devices of an embodiment is a sensor.

The gateway of an embodiment is connected to the LAN at the first location, and the LAN is coupled to a wide area network via a router at the first location.

The gateway of an embodiment is coupled to a wide area network and is coupled to the LAN at the first location via a router at the first location.

The gateway of an embodiment is coupled to a security server via the internet, the security server located at a second location different from the first location, the touchscreen providing interactivity with networked content of a remote network via the security server.

The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network from remote client devices.

The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

The gateway of an embodiment automatically discovers the security system components.

The gateway of an embodiment uses protocols of the security system to discover the security system components.

The gateway of an embodiment automatically establishes a coupling with the security system including the security system components.

The gateway of an embodiment includes a rules component that manages rules of interaction between the gateway and the security system components.

The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The secondary communication link of an embodiment includes a broadband coupling.

The secondary communication link of an embodiment includes a cellular coupling.

The gateway of an embodiment transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The gateway of an embodiment receives control data for control of the security system components from remote client devices via the secondary communication link.

The security network of an embodiment comprises network devices coupled to the gateway via a wireless coupling.

The gateway of an embodiment automatically discovers the network devices.

The gateway of an embodiment automatically installs the network devices in the security network.

The gateway of an embodiment automatically configures the network devices for operation in the security network.

The gateway of an embodiment controls communications between the network devices and the security system components.

The gateway of an embodiment transmits event data of the network devices to remote client devices over at least one of a plurality of communication links.

The gateway of an embodiment receives control data for control of the network devices from remote client devices via at least one of the plurality of communication links.

The event data of an embodiment comprises changes in device states of the network devices, data of the network devices, and data received by the network devices.

Embodiments of the integrated security system include a system comprising: a gateway at a first location, the gateway coupled to a local area network (LAN) and a security system of the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system, the gateway forming a security network that integrates functions of the security system with the LAN; an input/output (I/O) device at the first location and coupled to the gateway, the I/O device providing control of functions of the security system and the LAN; and a security server located at a second location different from the first location, the security server coupled to the gateway, the I/O device providing interactivity with networked content of a remote network via the security server.

Embodiments of the integrated security system include a system comprising: a gateway at a first location, the gateway coupled to a security system of the first location, the security system including a plurality of security system components that are proprietary to the security system, the gateway forming a security network that integrates functions of the security system with network devices of a local area network (LAN) of the first location; a touchscreen coupled to the gateway at the first location, the touchscreen providing control of functions of the security system and the network devices; and a security server located at a second location different from the first location, the security server coupled to the gateway, the touchscreen providing interactivity with networked content of a remote network via the security server.

Embodiments of the integrated security system include a system comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; a plurality of interfaces coupled to the processor and presented to a user via the touchscreen, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN; and a security server coupled to the touchscreen and the remote network, the security server located at a second location different from the first location.

The touchscreen of an embodiment provides interactivity with networked content of the remote network via the security server.

The touchscreen of an embodiment integrates the content with the access and the control of the security system.

The content of an embodiment includes interactive content.

The network interface of an embodiment allows the user to transfer content to and from the LAN.

The network interface of an embodiment allows the user to control functions of network devices coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides interactivity with a plurality of network devices coupled to the LAN.

The security system of an embodiment comprises a plurality of security system components, wherein the security interface provides the user with communication and control of the plurality of security system components.

The remote network of an embodiment is the internet and the network interface is a web browser.

The touchscreen of an embodiment integrates an internet browser and a security system control panel of the security system.

The system of an embodiment comprises an application engine coupled to the touchscreen, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A plurality of devices of an embodiment are coupled to the touchscreen.

The plurality of devices of an embodiment are coupled to the touchscreen via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the remote network.

The plurality of applications of an embodiment are accessed and loaded directly via the remote network.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between a plurality of devices comprising at least one of the security system components, devices coupled to the LAN, and devices coupled to the remote network.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The system of an embodiment comprises a first application engine coupled to the touchscreen, wherein the first application engine executes a security application that provides the security interface. The system of an embodiment comprises a second application engine coupled to the touchscreen, wherein the second application engine executes a content application that provides the network interface.

The system of an embodiment comprises a core engine coupled to the touchscreen, the core engine controlling dynamic provisioning of a plurality of applications and the content, the plurality of applications corresponding to the plurality of interfaces.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The touchscreen of an embodiment is coupled to the remote network via a broadband coupling.

The touchscreen of an embodiment is coupled to the remote network via a cellular coupling.

A plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

A device of the plurality of devices of an embodiment is a sensor.

The touchscreen of an embodiment is connected to the LAN at the first location, and the LAN is coupled to a wide area network via a router at the first location.

The touchscreen of an embodiment is coupled to a wide area network and is coupled to the LAN at the first location via a router at the first location.

The gateway of an embodiment is coupled to the security server via the internet, the touchscreen providing interactivity with networked content of a remote network via the security server.

The system of an embodiment comprises a portal coupled to the security server, wherein the portal allows control of the functions of the security system from remote client devices.

The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

The touchscreen of an embodiment automatically discovers security system components of the security system.

The touchscreen of an embodiment uses protocols of the security system to discover the security system components.

The touchscreen of an embodiment automatically establishes a coupling with the security system.

The touchscreen of an embodiment includes a rules component that manages rules of interaction with the security system.

The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the security system comprises security system components, wherein the touchscreen is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

The touchscreen of an embodiment transmits event data of the security system to the central monitoring station over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The secondary communication link of an embodiment includes a broadband coupling.

The secondary communication link of an embodiment includes a cellular coupling.

The touchscreen of an embodiment transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The touchscreen of an embodiment receives control data for control of the security system components from remote client devices via the secondary communication link.

Embodiments of the integrated security system include a system comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; a plurality of applications coupled to the processor, the plurality of applications displaying a plurality of interfaces to a user via the touchscreen, the plurality of interfaces including a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN; and a security server coupled to the touchscreen and the remote network, the security server located at a second location different from the first location.

Embodiments of the integrated security system include a system comprising: an input/output (I/O) device at a first location, the I/O device comprising a processor coupled to a local area network (LAN) and a security system at the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system; a security application coupled to the processor, the security application providing a security interface for control of functions of the security system, the security interface presented to a user via the I/O device; a content application coupled to a processor, the content application providing a network interface for access to networked content of a remote wide area network (WAN), the network interface presented to a user via the I/O device, wherein the I/O device is coupled to the WAN via the LAN; and a security server coupled to the I/O device and the WAN, the security server located at a second location different from the first location.

Embodiments of the integrated security system include a method comprising: coupling a touchscreen including a processor to a local area network (LAN) and a security system at a first location; and providing a plurality of interfaces to a user via the touchscreen, the plurality of interfaces coupled to the processor, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a wide area network (WAN) coupled to the LAN.

The touchscreen of an embodiment integrates the content with the access and control of the security system.

The content of an embodiment includes interactive content.

The network interface of an embodiment allows the user to transfer content to and from the LAN.

The network interface of an embodiment allows the user to control functions of peripheral devices of the first location coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides the user with communication and control of a plurality of network devices coupled to the LAN.

The network interface of an embodiment provides the user with communication and control of a plurality of security system components, wherein the security system comprises the plurality of security system components.

The WAN of an embodiment is the internet and the network interface of an embodiment is a web browser.

The touchscreen of an embodiment integrates a security system control panel and an internet browser.

The method of an embodiment comprises an application engine coupled to the processor, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

The plurality of devices of an embodiment are coupled to the processor.

The plurality of devices of an embodiment are coupled to the processor via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the WAN.

The plurality of applications of an embodiment are accessed and loaded directly via the WAN.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between the plurality of devices.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The method of an embodiment comprises a first application engine coupled to the processor, wherein the first application engine executes a security application that provides the security interface. The method of an embodiment comprises a second application engine coupled to the processor, wherein the second application engine executes a content application that provides the network interface.

The method of an embodiment comprises a core engine coupled to the processor, the core engine controlling dynamic provisioning of the plurality of applications and the content.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The processor of an embodiment is coupled to the WAN via a broadband coupling.

The processor of an embodiment is coupled to the WAN via a cellular coupling.

The plurality of interfaces of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

A device of the plurality of devices of an embodiment is a sensor.

Embodiments of the integrated security system include a method comprising: coupling a touchscreen including a processor to a local area network (LAN) and a security system at a first location; and displaying a plurality of interfaces to a user via the touchscreen, the plurality of interfaces displayed by a plurality of applications coupled to the processor, the plurality of interfaces including a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN.

Embodiments of the integrated security system include a method comprising: coupling an input/output (I/O) device including a processor to a local area network (LAN) and a security system at a first location, wherein the security system includes a plurality of security system components that are proprietary to the security system; providing a security interface for control of functions of the security system, the security interface presented to a user via the I/O device, wherein a security application coupled to the processor generates the security interface; and providing a network interface for access to networked content of a remote network, the network interface presented to a user via the I/O device, wherein a content application coupled to the processor generates the network interface.

Aspects of the integrated security system and corresponding systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including programmable logic devices (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects of the integrated security system and corresponding systems and methods include: microcontrollers with memory (such as electronically erasable programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the integrated security system and corresponding systems and methods may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

It should be noted that any system, method, and/or other components disclosed herein may be described using computer aided design tools and expressed (or represented), as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., HTTP, FTP, SMTP, etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of the above described components may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of "including, but not limited to." Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words "herein," "hereunder," "above," "below," and words of similar import, when used in this application, refer to this application as a whole and not to any particular portions of this application. When the word "or" is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

The above description of embodiments of the integrated security system and corresponding systems and methods is not intended to be exhaustive or to limit the systems and methods to the precise forms disclosed. While specific embodiments of, and examples for, the integrated security system and corresponding systems and methods are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the systems and methods, as those skilled in the relevant art will recognize. The teachings of the integrated security system and corresponding systems and methods provided herein can be applied to other systems and methods, not only for the systems and methods described above.

The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the integrated security system and corresponding systems and methods in light of the above detailed description.

In general, in the following claims, the terms used should not be construed to limit the integrated security system and corresponding systems and methods to the specific embodiments disclosed in the specification and the claims, but should be construed to include all systems that operate under the claims. Accordingly, the integrated security system and corresponding systems and methods is not limited by the disclosure, but instead the scope is to be determined entirely by the claims.

While certain aspects of the integrated security system and corresponding systems and methods are presented below in certain claim forms, the inventors contemplate the various aspects of the integrated security system and corresponding systems and methods in any number of claim forms. Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the integrated security system and corresponding systems and methods.

What is claimed is:

1. A system comprising:

a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location;

a plurality of user interfaces presented via the touchscreen, wherein the plurality of user interfaces include a security interface and a network interface, wherein the security interface provides control of functions of the security system and access to data collected by the security system, wherein the network interface provides access to data of devices of the LAN and a remote network coupled to the LAN; and

a security server coupled to the touchscreen and the remote network, the security server located at a second location different from the first location, wherein the security server comprises a client interface through which remote client devices exchange data with the security server, the security system, and the devices of the LAN.

2. The system of claim **1**, wherein the touchscreen provides interactivity with networked content of the remote network via the security server.

3. The system of claim **1**, wherein the touchscreen integrates the content with the access and the control of the security system.

4. The system of claim **1**, wherein the content includes interactive content.

5. The system of claim **1**, wherein the network interface allows the user to transfer content to and from the LAN.

6. The system of claim **1**, wherein the network interface allows the user to control functions of network devices coupled to the LAN.

7. The system of claim **1**, wherein the plurality of interfaces are configurable.

8. The system of claim **1**, wherein the network interface provides interactivity with a plurality of network devices coupled to the LAN.

9. The system of claim **1**, wherein the security system comprises a plurality of security system components, wherein the security interface provides the user with communication and control of the plurality of security system components.

10. The system of claim **1**, wherein the remote network is the internet and the network interface is a web browser.

11. The system of claim **1**, wherein the touchscreen integrates an internet browser and a security system control panel of the security system.

12. The system of claim **1**, comprising an application engine coupled to the touchscreen, wherein the application engine controls a plurality of applications executing under the processor.

13. The system of claim **12**, wherein the plurality of applications includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

14. The system of claim **12**, wherein the plurality of applications provides interactivity with a plurality of devices via the plurality of interfaces.

15. The system of claim **14**, wherein a plurality of devices are coupled to the touchscreen.

16. The system of claim **14**, wherein the plurality of devices are coupled to the touchscreen via a wireless coupling.

17. The system of claim **14**, wherein the plurality of devices include a plurality of devices of the security system.

18. The system of claim **14**, wherein the plurality of devices include a plurality of devices of the LAN.

19. The system of claim **14**, wherein the plurality of devices include a plurality of devices of the remote network.

20. The system of claim **14**, wherein the plurality of applications are accessed and loaded directly via the remote network.

21. The system of claim **12**, wherein the touchscreen includes the plurality of applications.

22. The system of claim **12**, wherein the plurality of applications includes a resident application that manages interactions between the plurality of applications.

23. The system of claim **22**, wherein the resident application manages interactions between a plurality of devices comprising at least one of the security system components, devices coupled to the LAN, and devices coupled to the remote network.

24. The system of claim **22**, wherein the resident application determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

25. The system of claim **24**, wherein the resident application allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

26. The system of claim **1**, comprising a first application engine coupled to the touchscreen, wherein the first application engine executes a security application that provides the security interface.

27. The system of claim **26**, comprising a second application engine coupled to the touchscreen, wherein the second application engine executes a content application that provides the network interface.

28. The system of claim **1**, comprising a core engine coupled to the touchscreen, the core engine controlling dynamic provisioning of a plurality of applications and the content, the plurality of applications corresponding to the plurality of interfaces.

29. The system of claim **28**, wherein the core engine manages images received from a plurality devices of at least one of the security system and the LAN.

30. The system of claim **29**, wherein the images include video.

31. The system of claim **1**, wherein the touchscreen is coupled to the remote network via a broadband coupling.

32. The system of claim **1**, wherein the touchscreen is coupled to the remote network via a cellular coupling.

33. The system of claim **1**, wherein a plurality of applications provides interactivity with a plurality of devices via the plurality of interfaces.

34. The system of claim **33**, wherein a device of the plurality of devices is an Internet Protocol device.

35. The system of claim **33**, wherein a device of the plurality of devices is a camera.

36. The system of claim 33, wherein a device of the plurality of devices is another touchscreen.

37. The system of claim 33, wherein a device of the plurality of devices is a device controller that controls an attached device.

38. The system of claim 33, wherein a device of the plurality of devices is a sensor.

39. The system of claim 1, wherein the touchscreen is connected to the LAN at the first location, and the LAN is coupled to a wide area network via a router at the first location.

40. The system of claim 1, wherein the touchscreen is coupled to a wide area network and is coupled to the LAN at the first location via a router at the first location.

41. The system of claim 1, wherein the gateway is coupled to the security server via the internet, the touchscreen providing interactivity with networked content of a remote network via the security server.

42. The system of claim 1, comprising a portal coupled to the security server, wherein the portal allows control of the functions of the security system from remote client devices.

43. The system of claim 42, wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

44. The system of claim 1, wherein the touchscreen automatically discovers security system components of the security system.

45. The system of claim 44, wherein the touchscreen uses protocols of the security system to discover the security system components.

46. The system of claim 1, wherein the touchscreen automatically establishes a coupling with the security system.

47. The system of claim 1, wherein the touchscreen includes a rules component that manages rules of interaction with the security system.

48. The system of claim 1, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the security system comprises security system components, wherein the touchscreen is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

49. The system of claim 48, wherein the touchscreen transmits event data of the security system to the central monitoring station over the secondary communication link.

50. The system of claim 49, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

51. The system of claim 48, wherein the secondary communication link includes a broadband coupling.

52. The system of claim 48, wherein the secondary communication link includes a cellular coupling.

53. The system of claim 48, wherein the touchscreen transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

54. The system of claim 53, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

55. The system of claim 48, wherein the touchscreen receives control data for control of the security system components from remote client devices via the secondary communication link.

56. A system comprising:

a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; and

a plurality of applications executing on the processor of the touchscreen, the plurality of applications displaying a plurality of user interfaces on the touchscreen, the plurality of user interfaces including a security interface and a network interface, wherein the security interface provides control of functions of the security system and access to data collected by the security system, wherein the network interface provides access to data of devices of the LAN and a remote network coupled to the LAN; and

a security server coupled to the touchscreen and the remote network, the security server located at a second location different from the first location, wherein the security server comprises a client interface through which remote client devices exchange data with the security server, the security system, and the devices of the LAN.

57. A system comprising:

an input/output (I/O) device at a first location, the I/O device comprising a processor coupled to a local area network (LAN) and a security system at the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system;

a security application executing on the processor of the I/O device, the security application providing a security user interface for control of functions of the security system, the security user interface presented via the I/O device;

a network application executing on a processor of the I/O device, the network application providing a network user interface that provides access to data of devices of the LAN and a remote wide area network (WAN), the network user interface presented via the I/O device, wherein the I/O device is coupled to the WAN via the LAN; and

a security server coupled to the I/O device and the WAN, the security server located at a second location different from the first location, wherein the security server comprises a client interface through which remote client devices exchange data with the security server, the security system, and the devices of the LAN.

58. A system comprising:

a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location;

a plurality of user interfaces presented via the touchscreen, wherein the plurality of user interfaces include a security interface and a network interface, wherein the security interface provides control of functions of the security system and access to data collected by the security system, wherein the network interface provides access to data of devices of the LAN and a remote network coupled to the LAN; and

a security server coupled to the touchscreen and the remote network, the security server located at a second location different from the first location, wherein the security server comprises a client interface through which remote client devices exchange data with the security server, the security system, and the devices of the LAN, wherein objects are maintained on the security server that correspond to at least one of at least one security system component of the security system and at least one network device of the LAN.

* * * * *

EXHIBIT 5

US008478871B2

(12) **United States Patent**
Gutt et al.

(10) **Patent No.: US 8,478,871 B2**
(45) **Date of Patent: *Jul. 2, 2013**

(54) **GATEWAY REGISTRY METHODS AND SYSTEMS**

(75) Inventors: **Gerald Gutt**, Tucson, AZ (US); **Aaron Wood**, Boulder Creek, CA (US)

(73) Assignee: **iControl Networks, Inc.**, Redwood City, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 299 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/637,671**

(22) Filed: **Dec. 14, 2009**

(65) **Prior Publication Data**

US 2010/0095369 A1 Apr. 15, 2010

Related U.S. Application Data

(63) Continuation of application No. 11/761,718, filed on Jun. 12, 2007, now Pat. No. 7,711,796.

(60) Provisional application No. 60/804,550, filed on Jun. 12, 2006.

(51) **Int. Cl.**
G06F 15/173 (2006.01)
G06F 15/177 (2006.01)

(52) **U.S. Cl.**
USPC **709/225**; 709/222

(58) **Field of Classification Search**
USPC 709/220–225
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,519,878	A	5/1996	Dolin, Jr.
D416,910	S	11/1999	Vasquez
5,991,795	A	11/1999	Howard et al.
6,219,677	B1	4/2001	Howard
6,286,038	B1	9/2001	Reichmeyer et al.
6,288,716	B1	9/2001	Humpleman et al.
D451,529	S	12/2001	Vasquez
6,331,122	B1	12/2001	Wu
6,363,417	B1	3/2002	Howard et al.
6,370,436	B1	4/2002	Howard et al.
6,377,861	B1	4/2002	York
6,400,265	B1	6/2002	Saylor et al.
D464,328	S	10/2002	Vasquez et al.
D464,948	S	10/2002	Vasquez et al.

(Continued)

FOREIGN PATENT DOCUMENTS

JP	2003-85258	A	9/2001
JP	2003-141659		10/2001

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 11/084,232 Office Action mailed Sep. 14, 2010.

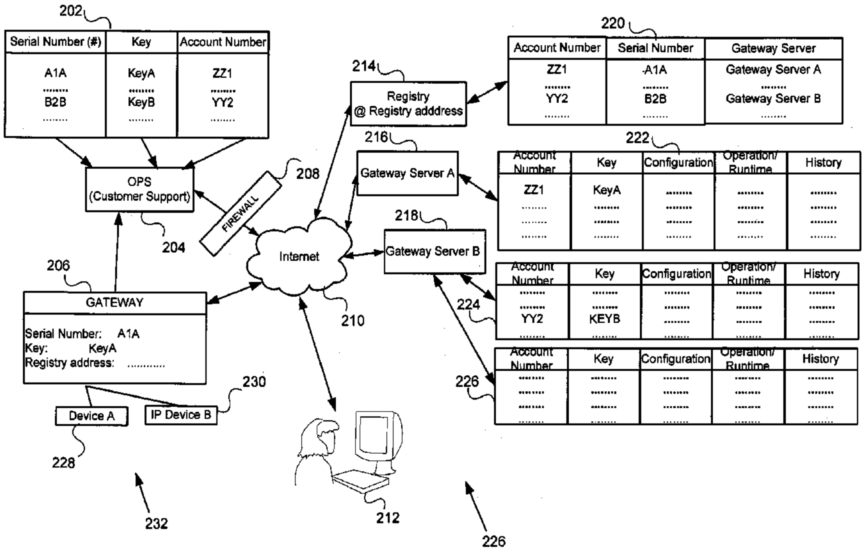
(Continued)

Primary Examiner — Joshua Joo
(74) *Attorney, Agent, or Firm* — Gregory & Sawrie LLP

(57) **ABSTRACT**

A gateway device for managing a set of two or more local management devices at a location. A system for networks at a plurality of locations. A method of operating a gateway device in a control network. A method for storing information to operate a gateway device in a control network. A method for storing information to operate a replacement gateway device in a control network.

43 Claims, 7 Drawing Sheets


202
Serial Number (#)
Key
Account Number
A1A
KeyA
ZZ1
B2B
KeyB
YY2
OPS
(Customer Support)
204
208
FIREWALL
Internet
210
206
GATEWAY
Serial Number: A1A
Key: KeyA
Registry address:
230
Device A
IP Device B
228
232
212
214
Registry
@ Registry adddress
216
Gateway Server A
218
Gateway Server B
220
Account Number
Serial Number
Gateway Server
Gateway Server A
Gateway Server B
222
Configuration
Operation/ Runtime
History
KeyA
224
KEYB
226

U.S. PATENT DOCUMENTS

6,462,663	B1	10/2002	Wilson et al.	
6,467,084	B1	10/2002	Howard et al.	
6,493,020	B1	12/2002	Stevenson et al.	
6,496,927	B1	12/2002	McGrane et al.	
6,529,723	B1	3/2003	Bentley	
6,542,075	B2	4/2003	Barker et al.	
6,563,800	B1	5/2003	Salo et al.	
6,574,234	B1	6/2003	Myer et al.	
6,580,950	B1	6/2003	Johnson et al.	
6,587,736	B2	7/2003	Howard et al.	
6,591,094	B1	7/2003	Bentley	
6,601,086	B1	7/2003	Howard et al.	
6,609,127	B1	8/2003	Lee et al.	
6,615,088	B1	9/2003	Myer et al.	
6,631,416	B2	10/2003	Bendinelli	
6,643,669	B1	11/2003	Novak et al.	
6,648,682	B1	11/2003	Wu	
6,661,340	B1	12/2003	Saylor et al.	
6,721,689	B2	4/2004	Markle et al.	
6,785,542	B1 *	8/2004	Blight et al.	455/426.1
6,965,313	B1	11/2005	Saylor et al.	
7,015,806	B2	3/2006	Naidoo et al.	
7,034,681	B2	4/2006	Yamamoto et al.	
7,082,460	B2 *	7/2006	Hansen et al.	709/220
7,113,090	B1	9/2006	Saylor et al.	
7,148,810	B2	12/2006	Bhat	
7,349,761	B1	3/2008	Cruse	
7,430,614	B2	9/2008	Shen et al.	
7,440,434	B2	10/2008	Chaskar et al.	
7,469,294	B1	12/2008	Luo et al.	
7,526,762	B1	4/2009	Astala et al.	
7,634,519	B2	12/2009	Creamer et al.	
2002/0026531	A1 *	2/2002	Keane et al.	709/250
2002/0029276	A1	3/2002	Bendinelli et al.	
2002/0083342	A1	6/2002	Webb et al.	
2002/0095490	A1	7/2002	Barker et al.	
2002/0103927	A1	8/2002	Parent	
2002/0107910	A1	8/2002	Zhao	
2002/0111698	A1	8/2002	Graziano et al.	
2002/0118107	A1	8/2002	Yamamoto et al.	
2002/0143923	A1	10/2002	Alexander	
2002/0180579	A1	12/2002	Nagoka et al.	
2002/0184301	A1	12/2002	Parent	
2003/0051009	A1	3/2003	Shah et al.	
2003/0062997	A1	4/2003	Naidoo et al.	
2003/0115345	A1	6/2003	Chien et al.	
2003/0132018	A1	7/2003	Okita et al.	
2003/0174648	A1	9/2003	Wang et al.	
2003/0187920	A1	10/2003	Redkar	
2003/0210126	A1	11/2003	Kanazawa	
2003/0236841	A1	12/2003	Epshteyn	
2004/0003241	A1	1/2004	Sengodan et al.	
2004/0015572	A1	1/2004	Kang	
2004/0103308	A1 *	5/2004	Paller	713/201
2005/0079855	A1	4/2005	Jethi et al.	
2005/0169288	A1	8/2005	Kamiwada et al.	
2005/0197847	A1	9/2005	Smith	
2005/0216302	A1	9/2005	Raji et al.	
2005/0216580	A1	9/2005	Raji et al.	
2006/0168178	A1 *	7/2006	Hwang et al.	709/223
2006/0181406	A1	8/2006	Petite et al.	
2007/0005736	A1 *	1/2007	Hansen et al.	709/220
2007/0052675	A1	3/2007	Chang	
2007/0106124	A1	5/2007	Kuriyama et al.	
2007/0286210	A1	12/2007	Gutt et al.	
2008/0147834	A1	6/2008	Quinn et al.	
2008/0180240	A1	7/2008	Raji et al.	
2008/0183842	A1	7/2008	Raji et al.	
2008/0235326	A1	9/2008	Parsi et al.	
2009/0204693	A1	8/2009	Andreev et al.	
2009/0240787	A1	9/2009	Denny	
2010/0082744	A1	4/2010	Gutt	
2010/0095111	A1	4/2010	Gutt	
2010/0095369	A1	4/2010	Gutt	

FOREIGN PATENT DOCUMENTS

JP	02-055895		2/2002
JP	2004-192659		2/2004
JP	H08-227491		9/2008
KR	2006-0021605		9/2004
WO	WO-2001-52478		7/2001
WO	WO-2001-99078		12/2001
WO	WO-2002-21300	A1	3/2002
WO	WO-2004-004222		1/2004
WO	WO-2004-107710		12/2004
WO	WO 2005/091218	A2	9/2005
WO	WO 2005/091218	A3	9/2005

OTHER PUBLICATIONS

EP 05725743.8 Supplemental Search Report mailed Sep. 14, 2010.
U.S. Appl. No. 12/630,092 Office Action mailed Jul. 21, 2010.
U.S. Appl. No. 12/019,568 Office Action mailed Jul. 13, 2010.
U.S. Appl. No. 12/019,554 Office Action mailed Jul. 12, 2010.
U.S. Appl. No. 12/019,554 Office Action mailed Jan. 5, 2010.
U.S. Appl. No. 11/761,745 Office Action mailed Apr. 13, 2010.
U.S. Appl. No. 11/084,232 Office Action mailed Dec. 30, 2009.
Alarm.com—Interactive Security Systems, Product Advantages, printed from website Nov. 4, 2003, 3 pp.
Alarm.com—Interactive Security Systems, Frequently Asked Questions, printed from website Nov. 4, 2003, 3 pp.
Alarm.com—Interactive Security Systems, Elders, printed from website Nov. 4, 2003, 1 page.
Alarm.com—Interactive Security Systems, Overview, printed from website Nov. 4, 2003, 2 pp.
X10—ActiveHome, Home Automation Made Easy!, printed from website Nov. 4, 2003, 3 pp.
Examination Report under Section 18(3) re UK patent application No. GB0724760.4 dated Jan. 30, 2008.
Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jan. 30, 2008.
Examination Report under Section 18(3) re UK patent application No. GB0724248.0 dated Jun. 4, 2008.
Examination Report under Section 18(3) re UK patent application No. GB0800040.8 dated Jan. 30, 2008.
Examination Report under Section 18(3), dated Aug. 13, 2007 re UK patent application No. GB0620362.4.

* cited by examiner

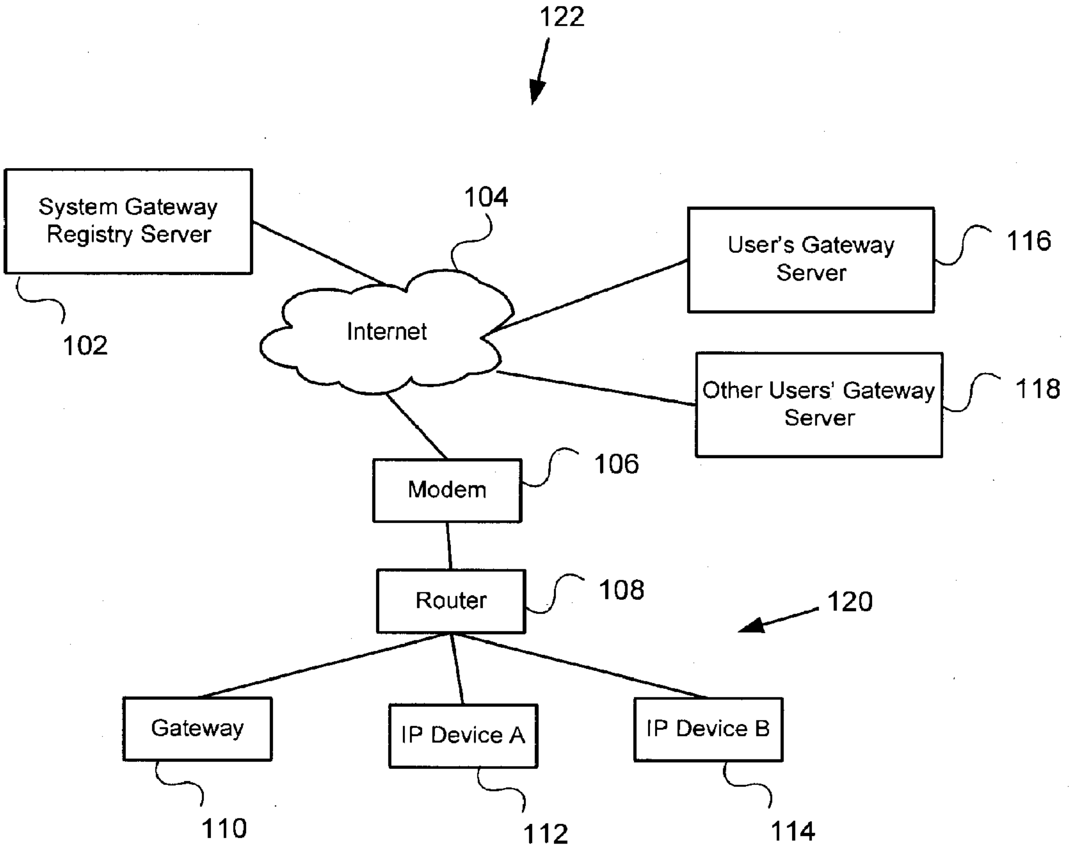

122
System Gateway Registry Server
102
104
Internet
User's Gateway Server
116
Other Users' Gateway Server
118
Modem
106
Router
108
120
Gateway
110
IP Device A
112
IP Device B
114

FIG. 1

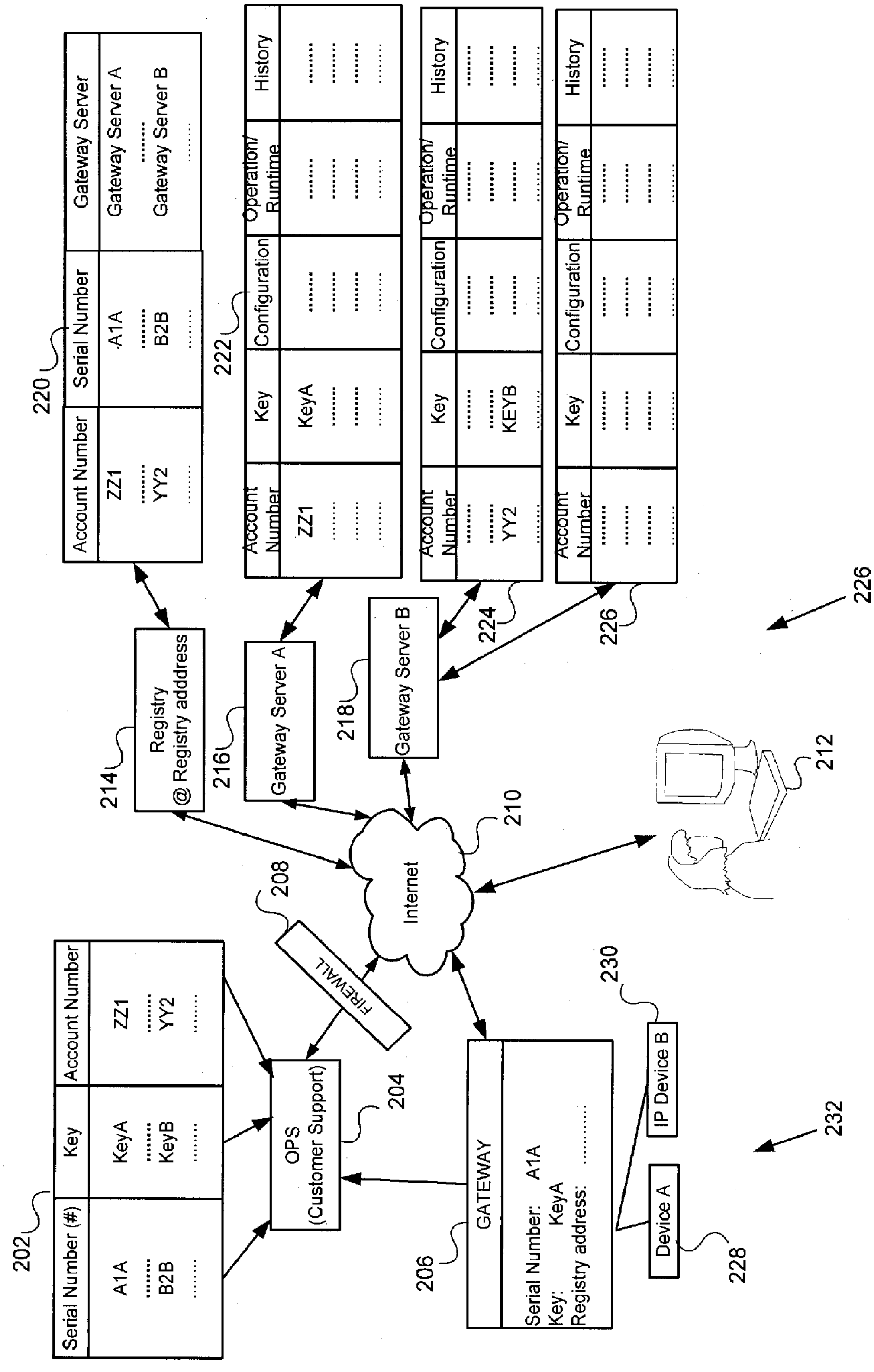

202
Serial Number (#)
A1A
B2B
Key
KeyA
KeyB
Account Number
ZZ1
YY2
OPS
(Customer Support)
204
FIREWALL
208
GATEWAY
Serial Number: A1A
Key: KeyA
Registry address:
206
Device A
228
IP Device B
230
232
Internet
210
212
Registry
@ Registry address
214
Gateway Server A
216
Gateway Server B
218
220
Account Number
ZZ1
YY2
Serial Number
A1A
B2B
Gateway Server
Gateway Server A
Gateway Server B
222
Account Number
ZZ1
Key
KeyA
Configuration
Operation/ Runtime
History
224
Account Number
YY2
Key
KEYB
Configuration
Operation/ Runtime
History
226
Account Number
Key
Configuration
Operation/ Runtime
History
226

FIG. 2

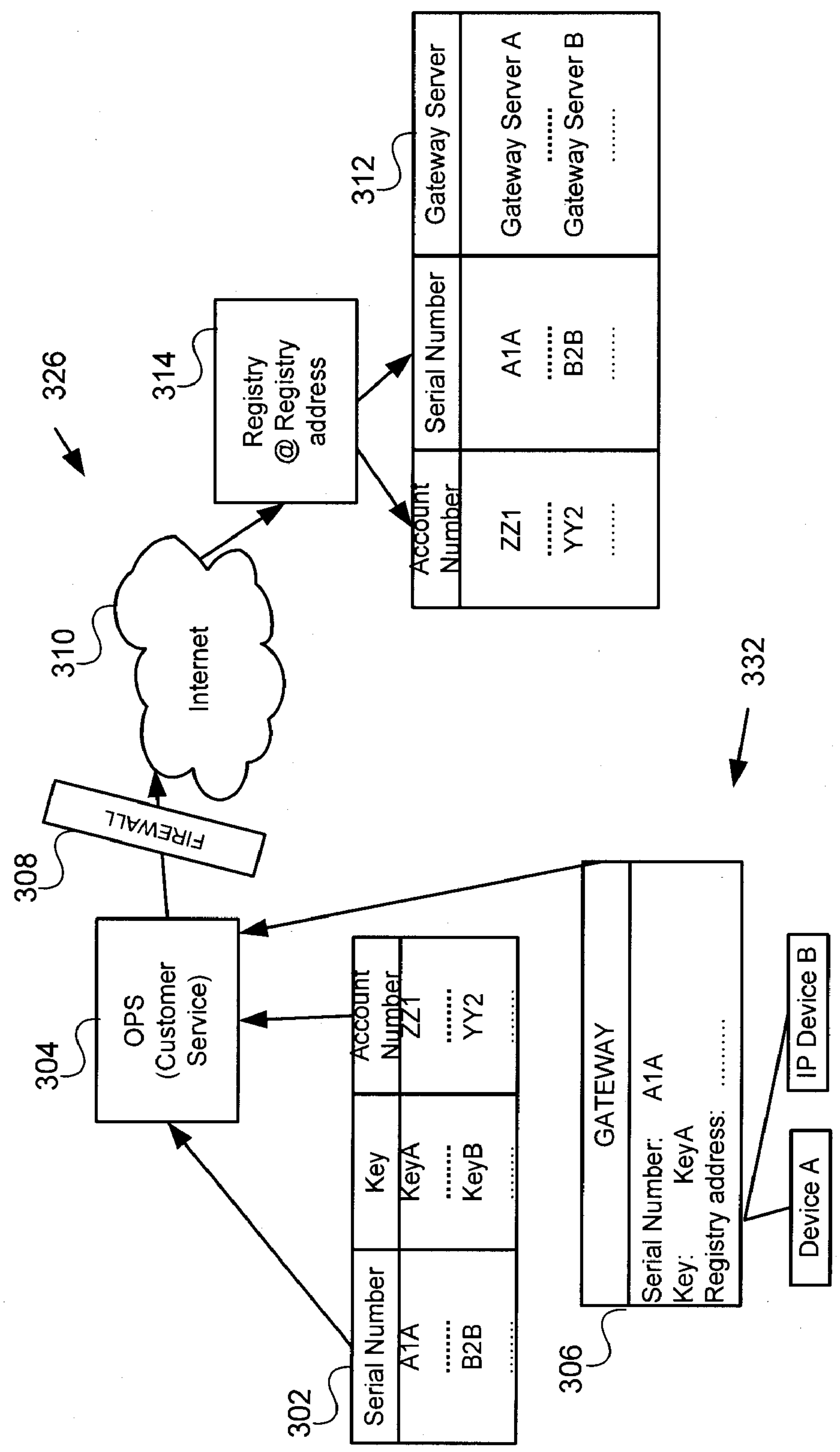

326
314
Registry
@ Registry address
312
Account Number
ZZ1
YY2
Serial Number
A1A
B2B
Gateway Server
Gateway Server A
Gateway Server B
310
Internet
308
FIREWALL
304
OPS (Customer Service)
302
Serial Number
A1A
B2B
Key
KeyA
KeyB
Account Number
ZZ1
YY2
306
GATEWAY
Serial Number: A1A
Key: KeyA
Registry address:
Device A
IP Device B
332

FIG. 3

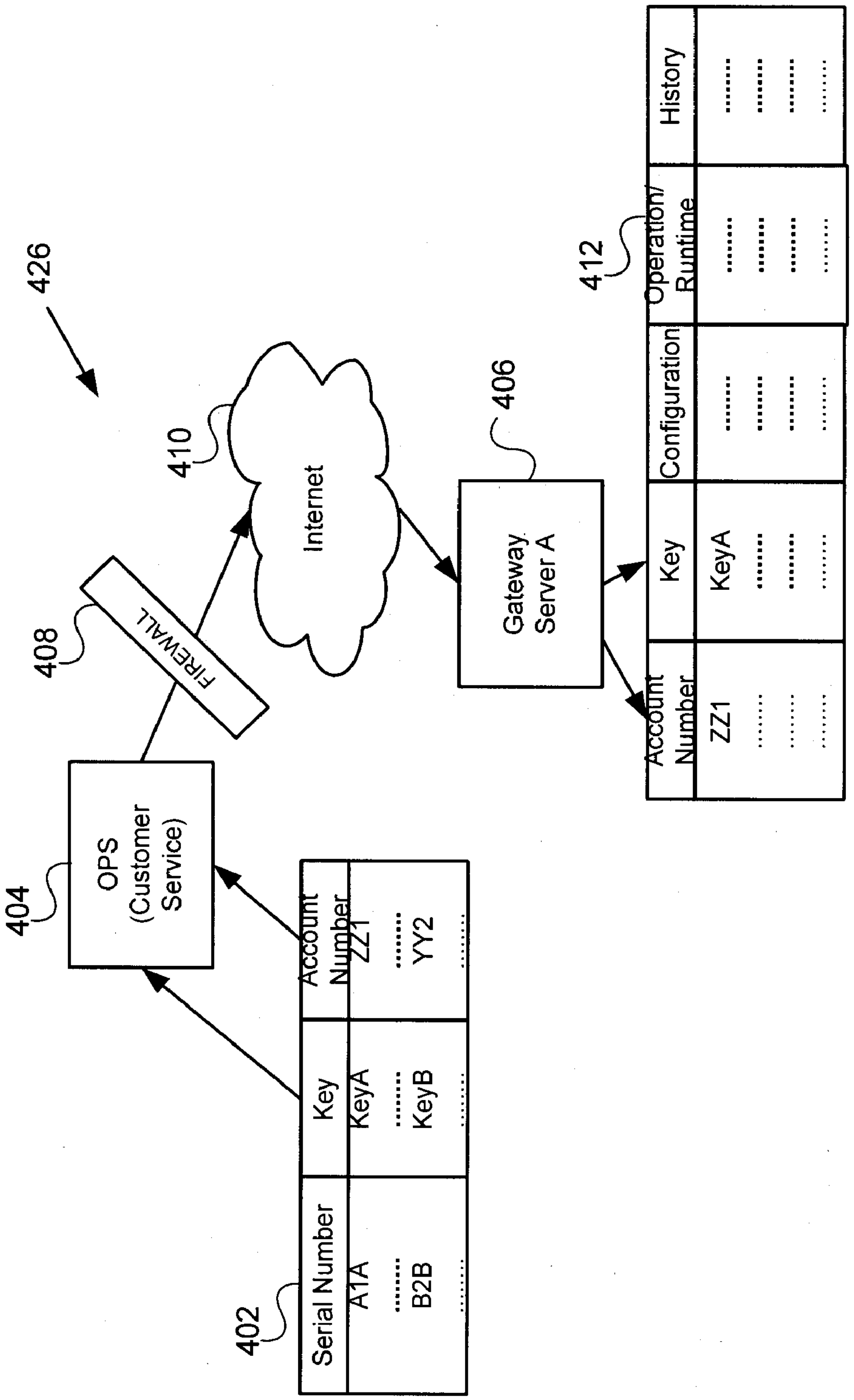

426
402
Serial Number
A1A
B2B
Key
KeyA
KeyB
Account Number
ZZ1
YY2
404
OPS (Customer Service)
408
FIREWALL
410
Internet
406
Gateway Server A
Account Number
ZZ1
Key
KeyA
Configuration
412
Operation/ Runtime
History

FIG. 4

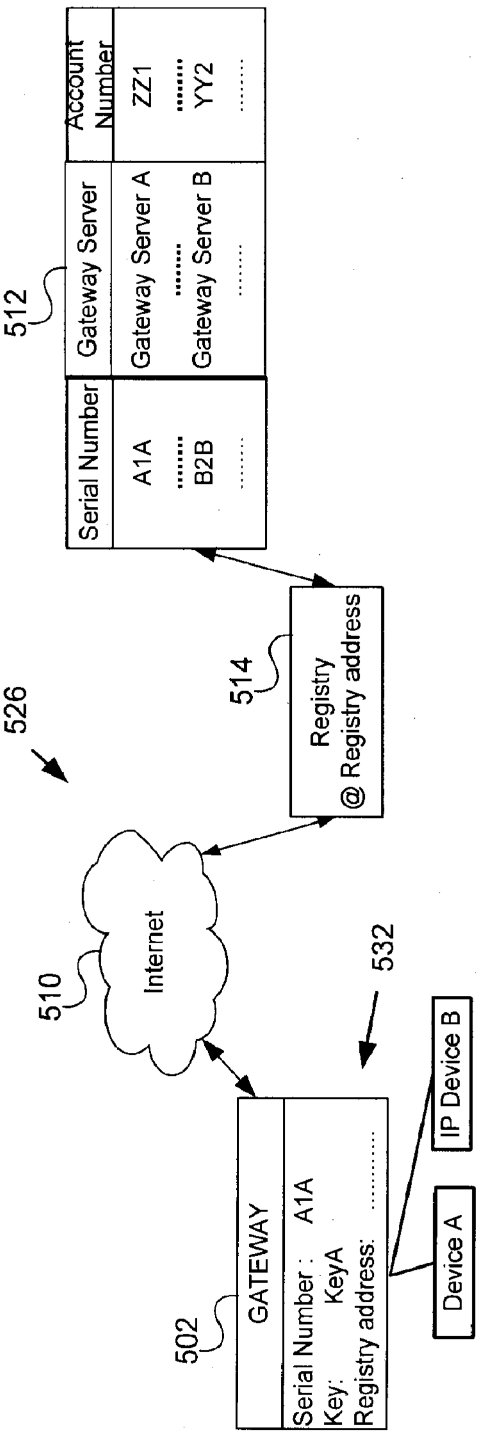

526
502
GATEWAY
Serial Number : A1A
Key: KeyA
Registry address: ....
Device A
IP Device B
532
510
Internet
514
Registry
@ Registry address
512
Serial Number
A1A
B2B
Gateway Server
Gateway Server A
Gateway Server B
Account Number
ZZ1
YY2

FIG. 5

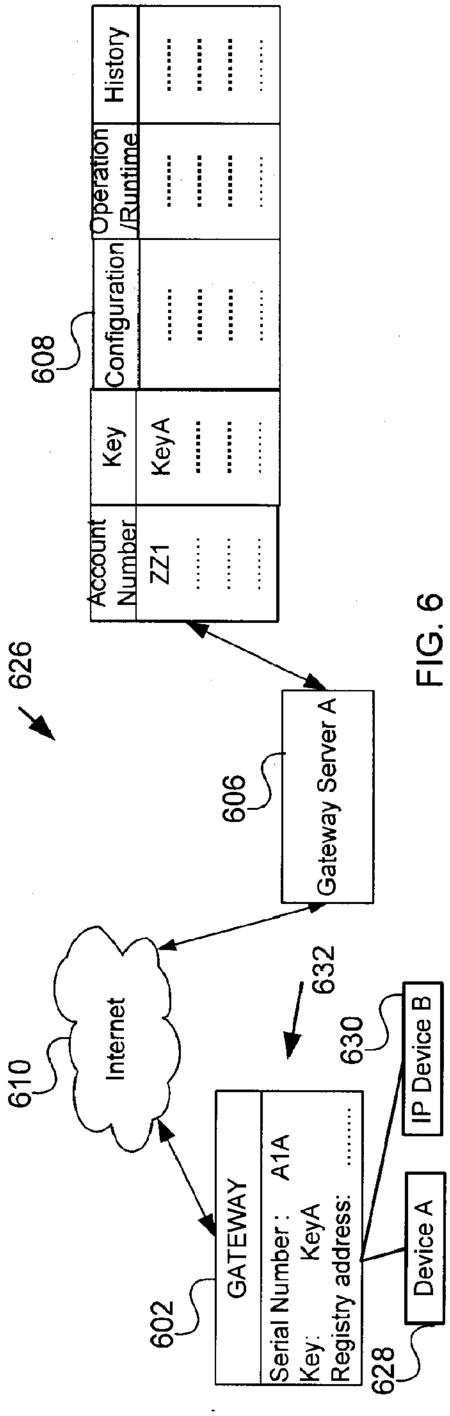

626
602
GATEWAY
Serial Number : A1A
Key: KeyA
Registry address: ....
628
Device A
630
IP Device B
632
610
Internet
606
Gateway Server A
608
Account Number
ZZ1
Key
KeyA
Configuration
Operation /Runtime
History

FIG. 6

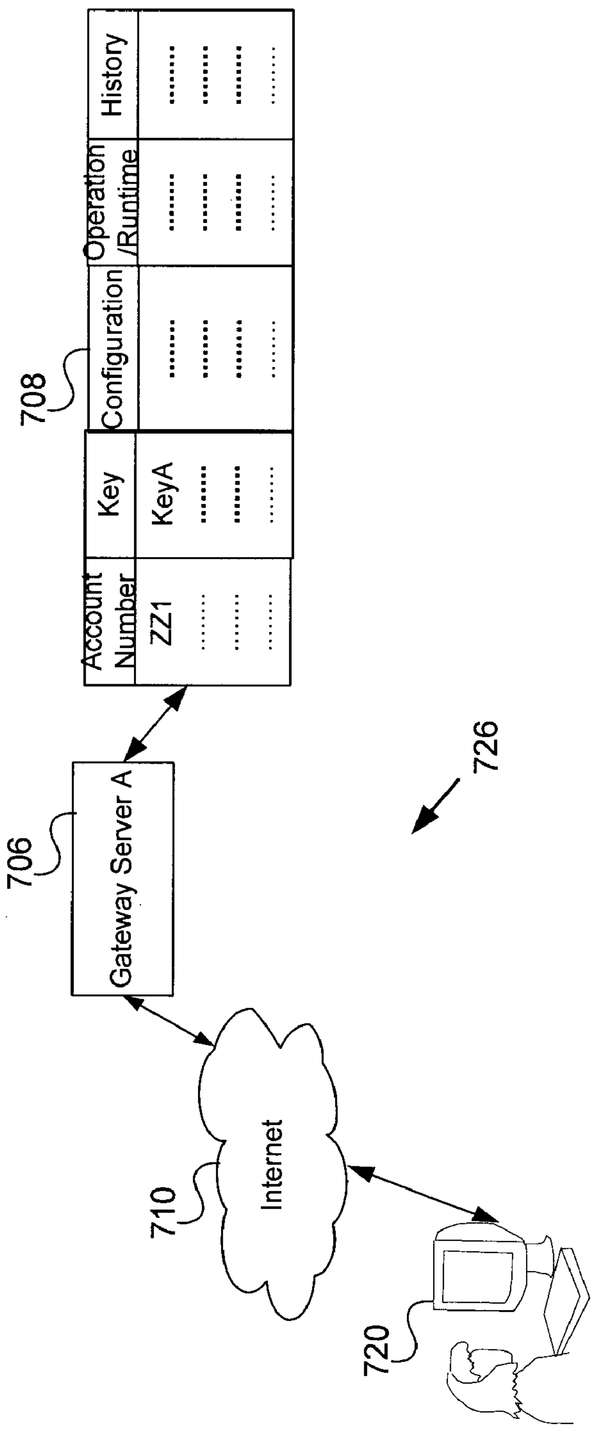

708
Account Number
Key
Configuration
Operation /Runtime
History
ZZ1
KeyA
706
Gateway Server A
726
710
Internet
720

FIG. 7

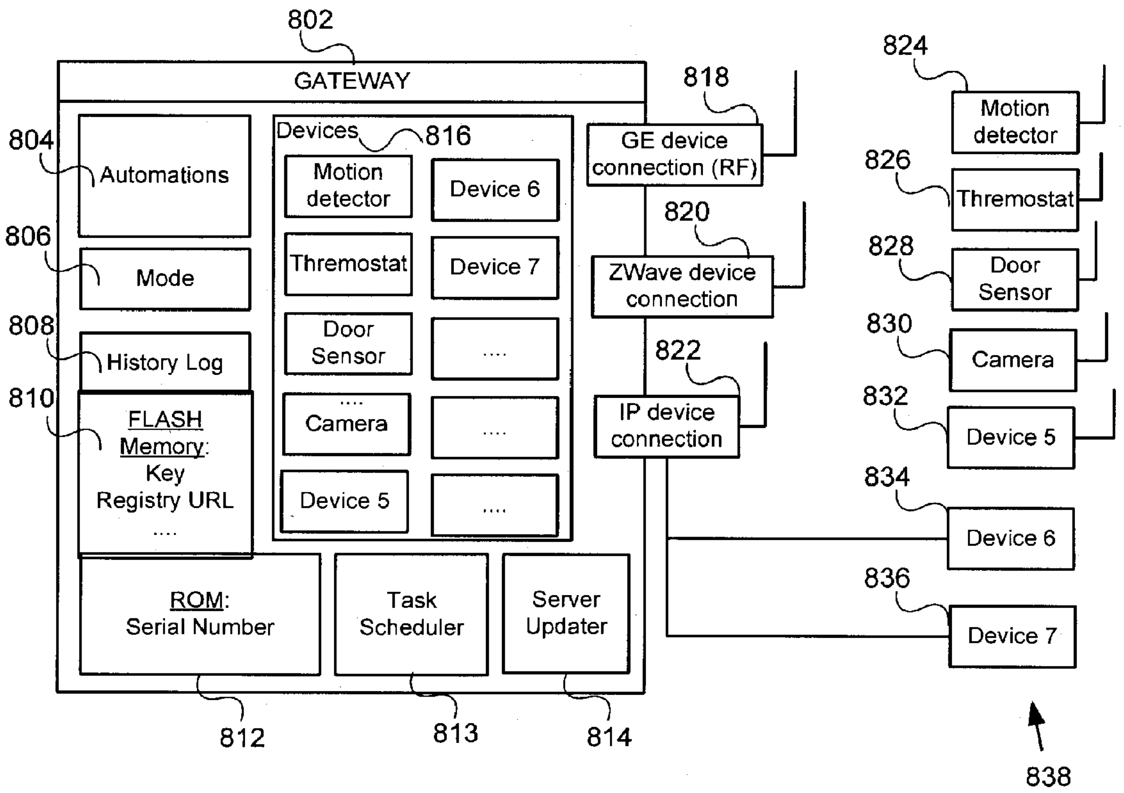

802
GATEWAY
804
Automations
806
Mode
808
History Log
810
FLASH Memory: Key Registry URL ....
Devices
816
Motion detector
Device 6
Thremostat
Device 7
Door Sensor
....
Camera
Device 5
ROM: Serial Number
Task Scheduler
Server Updater
812
813
814
818
GE device connection (RF)
820
ZWave device connection
822
IP device connection
824
Motion detector
826
Thremostat
828
Door Sensor
830
Camera
832
Device 5
834
Device 6
836
Device 7
838

FIG. 8

GATEWAY REGISTRY METHODS AND SYSTEMS

CROSS-REFERENCE

This application is a continuation of U.S. application Ser. No. 11/761,718, filed Jun. 12, 2007, which claims the benefit of U.S. Provisional Application No. 60/804,550, filed Jun. 12, 2006, the disclosures of which are hereby incorporated by reference in their entirety.

BACKGROUND

Vendors such as premises vendors, communication service vendors, and Internet portal vendors may desire to extend their relationship with vendees beyond the immediate transaction. Additionally, vendees desire additional premises management services beyond the immediate transaction for premises, communication services, or Internet portals. There is a need for advanced premises management services, methods, devices, and systems.

INCORPORATION BY REFERENCE

All publications and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication or patent application was specifically and individually indicated to be incorporated by reference. The following application incorporates by reference application Ser. No. 11/084,232, filed on Mar. 16, 2005 and application Ser. No. 11/084,657 filed on Mar. 16, 2005, in their entirety.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a system for managing control networks including a control network including a gateway, according to an embodiment.

FIG. **2** is a block diagram of a system for managing a set of control networks with gateway devices including a set of gateway servers, according to an embodiment.

FIG. **3** is a block diagram of a system for managing control networks showing management of keys, serial numbers and account numbers, according to an embodiment.

FIG. **4** is a block diagram of a system for managing control networks showing storage of account information, according to an embodiment.

FIG. **5** is a block diagram of a system for managing control networks showing initialization of a gateway device, according to an embodiment.

FIG. **6** is a block diagram of a system for managing control networks showing communication of a control network including a gateway device and a gateway server, according to an embodiment.

FIG. **7** is a block diagram of a system for managing control networks showing management of a control network, according to an embodiment.

FIG. **8** is a block diagram of a gateway device and showing location management devices, according to an embodiment.

DETAILED DESCRIPTION

While preferred embodiments of the present invention have been shown and described herein, such embodiments are provided by way of example only. Various alternatives to the embodiments of the invention described herein may be employed in practicing the invention.

Certain embodiments include methods, devices and systems for initializing and validating a system gateway device, also referred to as a gateway or a gateway device, which is used to manage a local network of location management devices at a location. The network and/or the devices may be managed using the gateway and can manage the network and/or devices from a location remote from the location of the devices and/or gateway. The location of the devices, for example, can be a premises such as a residence or business premises, and the devices including, for example, a thermostat or a camera, can be managed at the premises from a remote location such as, for example, from an office or using a cellular phone.

In some embodiments, the system gateway devices connect to servers (gateway servers) that contain the account information for the user of the system. The gateway itself does not necessarily know what server the account is on, and thus determines, is shown, or is told which server contains the account to manage the account remotely. The methods, systems, and devices provided herein make use of a gateway registry. The gateway registry communicates to the gateway the location of the server containing the account of the account associated with the gateway. The location may comprise, for example, the address of the server. A depiction of an embodiment of a gateway registry system is provided in FIG. **1**. FIG. **1** is a block diagram of a system **122** for managing control networks including a control network **120** including a gateway **110**, according to an embodiment. FIG. **1** shows IP devices **112**, **114** connected to router **108**, a gateway **110** connected to IP devices **112**, **114** through router **108** and connected through the router **108**, through modem **106**, and through Internet **104** to a central repository (the gateway registry **102**), two gateway servers **116**, **118** (user's gateway server **116** and another gateway server containing other users' accounts **118**), connected through Internet **104**, modem **106** and router **108** to gateway **110**.

Once the gateway server location is determined, and the gateway server is contacted, the gateway, in some embodiments, is validated by the gateway server in order for the gateway to gain access to the user account. Once this is done by the methods provided herein, and/or using the devices and/or systems provided herein, in order to manage the account, the gateway downloads the configuration for that account, wherein the configuration is in the account on the gateway server, and/or the gateway uploads data to the account from the premises in which it is installed.

In some embodiments, the configuration may be adjusted from a location remote to the premises where the local network that the gateway manages is located. In other embodiments, the configuration may be adjusted from the location of the premises where the local network that the gateway manages is located. In yet other embodiments, the configuration may be adjusted from either or both the location of the premises and/or from a remote location to the premises where the local network that the gateway manages is located.

For example, FIG. **2** is a block diagram of a system **226** for managing a set of control networks (for example, control network **232**) with gateway devices (for example, Device A **228**, IP device B **230**) including a set of gateway servers **216**, **218**, according to an embodiment. FIG. **2** depicts a user at a computer **212** connected to Internet **210**. Further depicted is a gateway device **206** comprising the serial number (serial #) of the gateway, which may be its MAC id or its Ethernet address, a key for the gateway, which may be installed by the manufacturer of the gateway, and the address of the registry, which may be a Uniform Resource Locator (URL) address for the registry server **214**. In the embodiment depicted in FIG. **2**, operational server (OPS) **204** is connected to database **202** (which may be called a master database or a table) which contains the serial numbers, keys and account identifications (which may be called account numbers) associated with gateways. OPS **204** is coupled to Internet **210** through a secure connection including firewall **208**. Master database **202** can be used to communicate to gateway registry **214** the serial number of the gateway **206**, the account number (or account identification) associated with the gateway, and/or the server address of the account associated with the gateway. Master database **202** can be used to communicate to the gateway server account information associated with the gateway, the gateway account number, and/or the key associated with the gateway. Gateway registry **214** of the embodiment depicted in FIG. **2**, is coupled to Internet **210**, and comprises a table **220** comprising the account number and gateway servers associated with gateways serial numbers. The table **220** of the Gateway registry **214** of the embodiment depicted in FIG. **2** also comprises the addresses and/or information about which gateway servers **216**, **218** connected to Internet **210** host the accounts associated with gateway account numbers and keys (which are associated with a gateway **206**). The Gateway servers **216**, **218** comprise tables **222**, **224**, **226** which contain account information associated with gateways (for example, gateway **206**). The account information in a table (for example table **222**) can be, for example, the account number of a gateway **206**, the key associated with a gateway **206**, configuration for devices **228**, **230** associated with a gateway **206**, operation time or run time associated with a gateway **206** or control network **232**, and history of the gateway **206**, devices **228**, **230** associated with the gateway **206** and/or the control network **232**, or the control network in general **232**. There may be several gateway servers, **216**, **218**, and there may be multiple tables (for example tables **224**, **226**) associated with a server (for example server **218**). Typically, an account associated with a gateway (for example gateway **206**) is located in a single table (for example table **222**) on a single server (for example server **216**). However, other arrangements are contemplated and described herein.

The keys may be protected and controlled such that only authorized devices, systems, and/or users may access the keys. The keys may be encrypted when transferred over an un-secure connection or a secure connection. The keys may be protected by a firewall. The accounts on the servers may, in some embodiments, comprise account configurations, operation time and/or run time information, and/or account history information.

The embodiment of FIG. **2** also shows example connections to and between each of the elements shown through which communication can be passed as described herein. The connections shown in FIG. **2** need not be physical connections, and elements and devices shown connected in FIG. **2** may be coupled together in another manner, such as through another device, or wirelessly, for non-limiting examples.

Provided herein are methods and systems by which a gateway can discover the server that hosts the user's account. Provided herein are gateway devices and/or systems which can discover the server that hosted the user's account.

Each gateway device contains a unique hardware address for its Ethernet connection. Ethernet devices have unique addresses, also called gateway device Ethernet addresses. The Ethernet address of a gateway device may be used as a unique serial number, or another combination of numbers and letters may be used as the unique serial number for a particular gateway. In some embodiments, the gateway stores the unique hardware address for initialization of the gateway device. At production time, or thereafter, a unique key is placed in, and stored in, the gateway device. Both the unique address and the unique key are also stored in a master database for subsequent linking to an account once the gateway is associated to an account, and/or for subsequent populating of a gateway registry table and/or subsequent populating of a gateway server table. The master database may be securely controlled with various levels of access allowed to authorized personnel only, for example, such as customer service personnel managing the master database. The master database may be protected by a firewall device (a firewall).

According to some embodiments, a central repository contains all known account numbers and the gateway unique numbers associated with the accounts. The location of the central repository is also stored by the gateway. In some embodiments the central repository is a gateway registry and/or gateway registry server of all known accounts and gateways. The gateway registry may also be populated with the gateway server information which may be known within the master database. Alternatively, the gateway server information may be known by a third party controlling the gateway server who communicates the server information to the registry directly, and the registry then records the server address associated with a particular account. In another embodiment, the gateway server information may be known by a third party controlling the gateway server who communicates the server information to the master database, directly or indirectly, and the master database then populates the registry with the server information associated with the account.

In some embodiments, the central repository (gateway registry) is populated using a secure connection to the Internet (firewall protected) with the account number associated with the gateway device and the serial number of the gateway associated with the account number and system

FIG. **3** is a block diagram of a system **326** for managing control networks (for example control network **332**) showing management of keys, serial numbers and account numbers, according to an embodiment. Shown in FIG. **3** are couplings between and information within and passed between gateway device **306**, operational server master database **302**, and gateway registry **314**. In the embodiment of FIG. **3**, the operational server (OPS) **304** and/or a customer service entity, upon association of a gateway device **306** to an account, populates a master database **302** with the account identification (which may be an account number) associated with the gateway device **306**, the serial number of the gateway **306** associated with the account identification, and the key associated with the gateway **306**. Operational server (OPS) **304** and/or a customer service entity, as shown in FIG. **3**, may also populate a table **312** of the gateway registry **314** using a secure coupling to Internet **310** (firewall **308** protected) with the account identification associated with the gateway device **306** and the serial number of the gateway **306** associated with the account identification.

According to some embodiments, upon association of a gateway device to an account (which is identified by the account identification, or account number), the gateway server may be populated with the account identification (or account number) associated with the gateway device and the key associated with the gateway device through use of the operational server (OPS) and/or a customer service entity. The master database of the OPS may provide the account identification associated with the gateway device, and/or the key of the gateway device to the gateway server.

In order to find the proper server to populate as described, in some embodiments, identification of the server that contains the account associated with the gateway device is performed by the OPS when the account identification and unique address is populated in the gateway registry. In some embodiments, the server information is temporarily stored in the master database, or temporarily stored by the OPS a sufficient amount of time to populate the server with the key associated with the gateway and the account number associated with the gateway device. In some embodiments, the server information is stored permanently in the master database when the gateway registry is populated by the master database. In some embodiments, the server is designated by the OPS. In some embodiments a third party or system that can manage the server and may or may not manage accounts on the server designates the server for an account.

In some embodiments, the gateway server information may be known by a third party controlling the gateway server who communicates the server information to the registry directly, and the registry then records the server address associated with a particular account. In another embodiment, the gateway server information may be known by a third party controlling the gateway server who communicates the server information to the master database, directly or indirectly, and the master database then populates the registry with the server information associated with the account.

For example, FIG. **4** is a block diagram of a system **426** for managing control networks (not shown) showing storage of account information, according to an embodiment. FIG. **4** depicts couplings between, and information within and passed between, operational server master database **402** and gateway server **406** using a method wherein operational server (OPS) **404** and/or a customer service entity uses master database **402** to populate a table **412** of a gateway server **406** using a secure connection to Internet **410** (firewall **408** protected) with the account identification (account number) associated with the gateway device, and with the key associated with the gateway device.

The central repository, in some embodiments a gateway registry and/or gateway registry server, of all known accounts and gateways is used to find which gateway server, called the account server and/or the gateway server, in some embodiments, holds the account information associated with the gateway (see, for non-limiting example, FIGS. **1** and **2**). While there may be several gateway registries existing, a gateway device knows only an address for, or location of, the gateway registry which contains its gateway unique address, account identification, and the gateway server address (or location), for the gateway server holding the account associated with the gateway device. In some embodiments, the gateway registry, registries, the gateway server, and/or gateway servers, are in different physical locations, and/or within different pieces of hardware. In some embodiments, the gateway registry, registries, the gateway server, and/or gateway servers, are conceptual locations, and/or logical constructs within a single piece of hardware. Various combinations of conceptual locations, logical constructs, physical locations, and different pieces of hardware are also contemplated herein for the gateway registry, registries, the gateway server, and/or gateway servers in some embodiments.

At power-on, the gateway device initializes, and sends a request to the central repository (for example, the gateway registry) specifying only the gateway unique address, for example a serial number for the gateway or the Ethernet address for the gateway. In some embodiments, the serial number for the gateway is the Ethernet address for the gateway. This address is then used to look up the user account associated with the gateway unique address, and respond back to the gateway device with the location of the server that it is to use to find the account associated with the gateway device. The gateway server at such location provided comprises the account associated with the gateway device which requested the information from the gateway registry. In some embodiments, the user account looked up is the account number associated with the unique address provided to the registry server. In other embodiments, the user account looked up is the account identification associated with the unique address provided to the registry server. The gateway server address received and the user account looked up are not sensitive, in that they are not, in and of themselves, sufficient to access the gateway server (as described herein), or to access the account on the gateway server associated with the gateway for which the unique address was provided.

For example, FIG. **5** is a block diagram of a system **526** for managing control networks (for example, control network **532**) showing initialization of a gateway device **502**, according to an embodiment. FIG. **5** is a block diagram depicting couplings between and information within a gateway device **502** and a gateway registry **514** used to execute a method of determining where the account associated with the gateway device **502** is located, and to determine the account number associated with the gateway **502**. In the embodiment shown in FIG. **5**, gateway **502** initializes, and sends a request to gateway registry **514** at the registry address stored in gateway memory, for example, in a table **512** of the registry **514**. The request to the registry specifies the serial number for the gateway stored in the table **512**. In the FIG. **5** embodiment, the serial number is used to look up the user account number associated with the gateway serial number, and the location of the server that contains the account associated with the gateway serial number. The registry **514** responds back to the gateway **502** with the account number (or account identification, in some embodiments) and location of the server that contains the account associated with the gateway. The gateway **502** stores the account number and the server location in its memory, in some embodiments.

At production time, in some embodiments, a unique key is placed in, and stored in, the gateway device. This key is then recorded by another repository, in some embodiments, the Operational Server, OPS, and/or a Customer Support Server. The key may be recorded as a key/value pair with the unique address of the device. The key may be the basis of an authentication that is used to validate that the gateway is the gateway for the user's account in order to access the account on the gateway server. In some embodiments, this key is used with a cryptographic hash to authenticate that the gateway is the correct gateway for the user's account. In some embodiments, this key is used with a cryptographic hash to create the authentication that the gateway is the correct gateway for the user's account. In some embodiments, this key is stored in the gateway device and the account identification looked up and received by the gateway from the gateway registry is used with a cryptographic hash to create the authentication that the gateway is the correct gateway for the user's account.

For example, FIG. **6** is a block diagram of a system **626** for managing control networks (for example control network **626**) showing communication of a control network **626** including a gateway device **602** and a gateway server **606**, according to an embodiment. FIG. **6** depicts a block diagram representation of an embodiment of the invention depicting couplings between and information within gateway device **602** and gateway server **606** used to execute methods for managing an account on the server **606** associated with the gateway device **602** and local management devices **628**, **630** on a local network **632** located at a location remote from the server **606**. In the embodiment shown in FIG. **6**, once gateway device **602** is communicated to with the location of the server **606** upon which the account resides associated with the gateway device **602** (i.e. hosting the account associated with the gateway device) and the account number (or account identification) associated with the gateway device **602**, the gateway device **602** sends an authentication based on the key stored in the gateway **602** and the account number (or account identification) stored in the gateway **602** to the server location of the server **606** hosting the account associated with the gateway **602**. If the authentication provided to server **606** by gateway **602** matches a server-generated authentication based on the key associated with the account number stored in memory server **608**, the gateway device **602** is allowed to access and manage the account associated with the gateway device on the server. This method, and devices and systems adapted to carry out this method validates that the gateway **602** is genuine, and not being impersonated by another device not authorized to manage or control the local network of devices **628**, **630** associated with the gateway **602**.

In some embodiments, the unique address to user account mapping is separate from the gateway key to user account mapping. In the first mapping, the gateway device uses the gateway serial number stored within the gateway device and the gateway registry location to contact the gateway registry in order to receive the location of the registry server and the account identification for the account associated with the gateway device. In the second mapping, the gateway device uses the location received from the registry to contact the gateway server and then uses the key stored on the gateway device and the account identification received from the registry as the bases for an authentication that unlocks the account associated with the gateway device to the gateway device.

Once the first mapping has occurred, in some embodiments, the gateway stores the location of the registry server and the account identification received by the registry in temporary memory which can be accessed so long as the gateway is not powered-off and/or does not lose power. In some embodiments, once the first mapping has occurred, the gateway stores the location of the registry server and the account identification received by the registry in permanent memory and is accessible by the gateway regardless of whether the gateway loses power or is powered-off.

Once a gateway server has been identified by a gateway device, and the gateway server has validated that the gateway is genuine per the methods and by devices and systems described herein, the network of local management devices coupled to the gateway at the location can be remotely managed from a location remote to the location of the gateway device and location management devices by viewing the account on the server through, for example, a remote network such as the Internet.

For example, FIG. **7** is a block diagram of a system **726** for managing control networks (not shown) showing management of a control network (not shown), according to an embodiment. FIG. **7** depicts couplings between a remote management device **720** capable of managing a network (not shown) of local management devices at a location remote from the remote management device **720**. In such embodiment, the remote management device **720** couples (through, for example, Internet **710**) to gateway server **706** containing a table **708** containing account information for the network of local management devices (not shown) associated with the gateway device (not shown) and with the account information in the table **708** on the gateway server **706**. The remote management device **720** thus may be used to manage and control the account information on the server **706**, which, as shown in FIG. **6** couples with the gateway device **602** at the location which couples to the local management devices **628**, **630** at the location. A user of the remote management device **720**, which may be a computer, PDA, cellular phone, or another device coupled to the Internet wirelessly or wired, may, for example, change configuration data in the table **708** of the server **706**, wherein the configuration data shows the current status of a device on the local network connected to the gateway associated with the account, such as the temperature in a particular room, or view the output of a camera in a child's room, or view the inside of a vault, or turn on a light, or unlock a door, or any combination of these and other activities. Other types of devices are provided and contemplated herein, any of which could be managed using the system, devices, and methods described herein.

FIG. **8** is a block diagram of a gateway device **802** and showing location management devices **824**, **826**, **828**, **830**, **832**, **834**, **836**, according to an embodiment. FIG. **8** shows an embodiment of a gateway device **802** coupled to a set **838** of network devices at a location. The gateway device embodiment shown in FIG. **8** is a block diagram depicting logical representations for each of the elements within the gateway device **802**, and a block representation of multiple local management devices **824**, **826**, **828**, **830**, **832**, **834**, **836** at the location which the gateway device **802** can manage and control. In the embodiment shown, gateway device **802** comprises logic **816** for managing which, for non-limiting example, can include monitoring and controlling, a set of local management devices **838** connected to a local network located at the location. The gateway device **802**, in some embodiments, is also located at the location and connected to the local network. The logic of the embodiment shown in FIG. **8** comprises, for non-limiting example, automations **804**, mode **806**, task scheduler **813**, and server updater **814**. The gateway device of this embodiment comprises an interface that allows connectivity to a remote network over which the gateway can communicate to remote systems which are remote to the location. Such remote systems may include a gateway server, a gateway registry, an operational server, a remote management device, as provided herein. The gateway device may also have an interface for communication to at least one local management device (for example, local management devices **824**, **826**, **828**, **830**, **832**, **834**, **836**), a processor (not shown), memory **810**, **812**, an address of a gateway registry (in this case, a URL, although other addresses are contemplated), a serial number of the gateway, and a key.

Although not shown, the gateway device **802** of the embodiment of FIG. **8** comprises logic that, upon initialization of the gateway uses the address of the gateway registry to communicate with the gateway registry, sends a request to the gateway registry specifying the serial number of the gateway, receives a response with an address of the server upon which an account associated with the gateway is stored, and receives a response with an identification of an account for managing the location associated with the gateway; and logic that communicates with the server upon which the account associated with the gateway is stored by using the identification and authentication information derived based on the key.

In the embodiment shown in FIG. **8**, devices **824**, **826**, **828**, **830**, **832**, **834**, **836** on the network that the gateway **802** can manage and control include, as non-limiting examples, a motion detector **824**, a thermostat **826**, a door sensor **828**, a camera **830**, and other local management devices (for non-limiting example, devices **832**, **834**, **836**). The gateway **802** is shown having conceptual placeholders **816** for devices (not the actual devices) within it. These conceptual placeholders **816** may, in some embodiments, store the settings, software, logic, and hardware for controlling and managing the actual devices which are external to the gateway at the location. The embodiment gateway in FIG. **8** can communicate to the devices by RF **818**, Z-wave **820**, and/or IP **822**, as non-limiting examples. In other embodiments, the gateway **802** can communicate to local management devices by any other communication means, including by wired and wireless means.

When the configuration data on the server is changed, the gateway which contains settings for each local management device at the location connected to it, can update its settings to conform to the server configuration by contacting the server and validating that it is the genuine gateway associated with the account stored in its memory, as described herein, and accessing and downloading the configuration settings or the changed configuration settings on the server for the account.

Provided herein is a method, system, and device wherein an account may be moved from server to server as needs change (moving data-centers, etc.) without having to update the gateway devices out in the field that the server has changed. The gateway can communicate with the central repository to find the new server location by executing the method done when initializing. For example, when the gateway server containing the account associated with a particular gateway is moved, the gateway which has already executed the first mapping will not be able to access its account using the server location stored in its memory. When the gateway contacts the gateway server at the location it previously received from the gateway registry, it receives an error message or a non-response from the gateway server, since there is no account identification on the gateway server matching the account identification provided by the gateway device. When such error or non-response is detected by the gateway, the gateway can re-initialize (repeat the first mapping), determine the new server location and re-receive the account identification from the gateway registry, per the methods and using the devices described herein.

Provided herein is a method and system wherein the account associated with the gateway device (called the previous gateway device) may be associated with a new gateway device. The new gateway can be associated with an existing account on a server by first updating the master database with the new gateway serial number and new gateway key, and by associating the new key and new serial number with the account identification formerly associated with the previous gateway device. The gateway registry may then be updated by using methods and systems described herein to populate the gateway registry table with the new gateway serial number and associating the new gateway serial number with the server address associated with the previous gateway device. The gateway server may then be updated by using methods and systems described herein to populate the gateway server table with the new gateway key and associating the new gateway key with the server address associated with the previous gateway device and associating the new key with the account identification associated with the previous gateway device. Once the gateway registry and the gateway server are updated to be associated with the new gateway device, upon initialization of the new gateway (such as upon powering-on), the new gateway device can use embodiments of the methods and systems provided herein to allow remote (and/or local) management of the local management devices to which it couples. It is contemplated that a new gateway device, which is also a gateway device, may comprise the various embodiments of the gateway device as described herein.

An embodiment allows the gateway to not have to (although it may) store any user account information other than its gateway serial number, logic to communicate with the devices to which it is connected based on account information received from the gateway server, memory, a processor, interfaces to the local network of local management devices and to the local management devices that the gateway manages, interface to systems on a network remote to the location of the local management devices that the gateway manages, and logic to carry out the mappings as described herein. In some embodiments, the systems comprise the gateway registry, and the gateway server. In some embodiments, the gateway stores history of the devices on the network managed by the gateway and/or history of the gateway.

The authentication provided by the gateway to the gateway server to access the account associated with the gateway may comprise a cryptographic hash of the key stored in the gateway. The authentication matches identical information stored on the gateway server, and allows the gateway server to ensure that the gateway device is genuine, and is not in fact another device/computer trying to masquerade as the user's gateway device.

The separately stored mappings between the account identification and the key, and the account serial number and the account identification of the gateway is a security measure to ensure that it is more difficult to break into either the gateway registry or the gateway server and discover the key and account identification pair, both of which may be used to operate correctly as the gateway.

For example, an embodiment of the invention comprises any of the above systems or methods alone or in combination as part of a network for premises management. The network may include premises management devices such as a smart thermostat. The premises management devices are connected to a premises network which can be, for example, an RF and/or power line network. The premises network is connected to a gateway which in turn is connected to a broadband device such as a DSL, cable, or T1 line. The gateway can alternatively or also be connected to a dial up modem. The premises is connected to the Internet according to an embodiment. The Internet is connected to system managers at the network operations center. The Internet is also connected to customers of the system manager, for example vendors such as premises vendors, communication service vendors, or Internet portal vendors. The Internet is also connected to vendees, such as premises vendees, communication service vendees, or Internet portal vendees.

An embodiment may include programmable code and devices with screens of a portal interface for premises management. For example, code with may summarize premises management services. Code may summarize security management services and safety management services. Code may also summarize energy management services. Services offered by the system can be branded and incorporated into a third part web portal, for example, in a personal portal such as one provided by Yahoo.

The look and feel of the system pane can be tailored by the service provider.

In an embodiment, a system portal summary page may show a snap-shot of the state of the various devices in the user premises. For example, in an embodiment, the user can change premises by clicking on this box and selecting a different premises. A status pane may list the different devices in the user premises along with their actual states. A pending updates pane may show the time of the last communication between the premises and the server as well as any pending updates waiting to be sent downlink to the premises. The pictures pane shows the last several (e.g., last four) pictures taken by the camera in the user premises. The user can click on a thumbnail picture to look at a larger version of the photo as well as access archived images for that camera, look at live video, take new pictures or delete photos. The schedule pane shows the scheduled activities for the premises. The alarm history shows an archive of the most recent event and activity in the user premises. The reminders pane provides a means for the system to remind the user to perform certain activities or functions related to their home or business. The mode drop down button on the respective navigation bar allows the user to switch between the systems modes. The QuikControl drop down allows the user to control any device that is controllable (e.g., camera, thermostat, lamps, etc.).

According to an embodiment, a method is provided for premises management networking. Premises management devices connected to a gateway at a premises are monitored and controlled. According to an embodiment, an uplink-initiation signal associated with a network operations center server is received at the premises. In response to the uplink-initiation signal, communications between the gateway and the network operations center server may be initiated from the gateway at the premises. During the communications between the gateway and the network operations center server, information associated with the premises management devices may be communicated.

The premises gateway can be a low-cost and standalone unit that connects the in-premises devices to the server. The connectivity to the Internet can be accomplished via a broadband connection (Digital Signal 1 (T1), Digital Subscriber Line (DSL) or cable) and/or via the telephone line. Though broadband connectivity may be used, telephone connectivity may be present as a back-up option in case the broadband connection is lost. For premises without a broadband connection (e.g., vacation homes) a telephone-only connection can be used.

A user account may be established by the end user using personal information (name, payment option, etc.) of the user. The account registration may involve the user logging on to the system manager web site and establishing a new account by entering name, address, phone number, payment details and/or the gateway serial number printed on the gateway in the end user's possession. In some cases the system manager service account may already be pre-established with the gateway serial number and the end user simply has to update the account with personal and payment information. Multiple gateways can also be handled per user account.

The gateway may be registered to associate the user account on the system manager server (established in the previous step) with an actual gateway in the user's home. The gateway is connected to a broadband network or the telephone line in the home.

An embodiment may help provide users with a hosted and managed service for premises device monitoring and control for a fee, such as a monthly subscription fee. The premises markets include residential homes, commercial multiple tenant units (MTUs) as well as small businesses.

Embodiments may provide device logging, activity logging and tracking. For example, an embodiment can log any device variable specified by the user for up to, for example, 30 days. The user defines a logging interval for each variable at the time of configuration. The logging feature can be handled by the gateway on the local device side and the data can be transferred to the server at regular intervals. The overall variable log for all variables can be kept on the server side. Logging of data for more than, for example, 30 days (but no more than, for example, 180 days) can be provided to the user, for example for a nominal fee. An embodiment may provide at least, for example, a 14-day history log of all user, system and device actions. An action includes a change to a device variable, system or network settings brought on by either the system or the user (e.g., variable changed, logging enabled, device added, user notified, etc.). The user can trace back system activities to their cause and to the date and time they occurred. Past activities can be searched by variable, device, category or date.

An embodiment can support user-defined modes, such as "home," "away," "sleep," "vacation," etc. The mode the user network is in plays a factor in the determination of the actions taken (reporting, alarming, eventing, notification, etc.) by the system when variable changes occur. According to an embodiment, the user can specify alarm conditions for variables with discrete states (e.g., binary ON/OFF). These alarms can be reported in real-time (i.e., immediate uplink) by the gateway to the server. The server then in turn looks at the data and determines, based on user alarm settings, whether to notify the user or not.

According to an embodiment, for non-critical events, the system can notify the user in non-real-time fashion regarding the state of any variable specified by the user. The variables chosen for user eventing can be of any kind (discrete or continuous). The gateway updates the server with the change of variable state/value at a regularly scheduled upload. The server continuously looks at variable data and determines, based on user eventing settings, whether to notify the user or not. Eventing conditions can be determined based on the value or state of a variable as well as the system mode. According to an embodiment, the system can support user alarming and eventing via the following methods: email, text messaging, pager, and/or voice telephone call (voice synthesis).

An embodiment may provide device data monitoring and control. The user can specify any device variable for monitoring and control via the server portal. For example, up to 255 devices can be supported by a single gateway. For example, up to 512 variables can be supported by a single gateway.

The system can support an open architecture where most, if not all device networking protocols can be supported. Examples of specific device protocols supported by the system include RF and powerline protocols, such as GE Interlogix RF and Echelon LonWorks power line (PL & FT), simplifying the installation burden by requiring no new wires to be installed in a premises. The LonWorks free topology twisted pair medium (FT-10) can be supported as an option to support certain commercial applications (e.g., office buildings).

The following is a non-exhaustive list of a few other devices supported by the system.

1. Small data/message display—for text messages, news, weather, stock, photos, etc.
2. Door latch control
3. Pool/spa control
4. Weather station
5. Lighting control
6. Elderly or disabled monitoring
7. Irrigation controller (Bibija)
8. VCR programming

The system can support cameras. For example, standard off-the-shelf IP cameras (also referred to as web cameras) may be used, such as those available from vendors such as Axis, Panasonic, Veo, D-Link, and Linksys, or other cameras manufactured for remote surveillance and monitoring. Surveillance cameras may contain a standalone web server and a unique IP address may be assigned to the camera. The user of such a camera would typically retrieve the camera image by accessing the camera's web page through a standard web browser, using the camera's IP address. In some cases the IP camera acquires a local IP address by using a Dynamic Host Configuration Protocol (DHCP) client to negotiate an address from the local DHCP server (usually residing in the user's router/firewall).

According to an embodiment, a gateway can initiate all communications with the server. Gateway communication can either initiate based on a predetermined schedule (e.g., every 30 minutes) or due to a local premises alarm (selected by the user).

Gateways can contact a common server for their first uplink connection in order to obtain their assigned gateway server address, which they can use for all subsequent uplink connections (unless changed later by the system). In the event that the gateway cannot connect to its designated gateway server, it can fall back to contacting the default initial gateway in order to refresh its gateway server address.

The predetermined call initiation schedule can be programmable by the server and can provide different intervals for broadband and telephone intervals (e.g., every 30 minutes for broadband and every 90 minutes for telephone).

An embodiment may be directed to a control network having a collection of sensor and actuator devices that are networked together. Sensor devices sense something about their surroundings and report what they sense on the network. Examples of sensor devices are door/window sensors, motion detectors, smoke detectors and remote controls.

Actuator devices receive commands over the network and then perform some physical action. Actuator devices may include light dimmers, appliance controllers, burglar alarm sirens and cameras. Some actuator devices also act as sensors, in that after they respond to a command, the result of that command is sent back over the network. For example, a light dimmer may return the value that it was set to. A camera returns an image after has been commanded to snap a picture.

In addition to the foregoing, the following are various examples of embodiments of the invention.

Some embodiments of a method for premises management networking include monitoring premises management devices connected to a gateway at a premises; controlling premises management devices connected to the gateway at the premises; receiving, at the premises, an uplink-initiation signal associated with a network operations center server; and in response to the uplink-initiation signal, initiating, from the gateway at the premises, communications between the gateway and the network operations center server; and communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices.

The uplink-initiation signal can be received via telephone and/or broadband connection. The gateway can initiate communications between the gateway and the network operations center server with at least a Hypertext Transfer Protocol (HTTP) message and/or at least an Extensible Markup language (XML) message. The premises management devices can manage energy of the premises, security of the premises, and/or safety of the premises. Many embodiments provide a hosted solution for property developers, owners and managers as well as service providers (Internet Service Providers (ISPs), telcos, utilities, etc.) such as communication service providers and Internet portal providers. Some embodiments offer a complete, turnkey, reliable, and/or cost-effective solution for the delivery of telemetry services (e.g., energy management, security, safety, access, health monitoring, messaging, etc.) to customers.

An embodiment of the invention is directed to a business method for premises management. Some embodiments of a business method for premises management include making an Internet portal available for access to a vendee, such as a premises vendee, communication service vendee, and/or an Internet portal vendee; and at least after a transaction between the vendor and the vendee, such as a premises transaction, a communication services transaction, and/or Internet portal services transaction, providing premises management services via the Internet portal to the vendee.

The Internet portal can be branded with a brand of the vendor according to an embodiment. Examples of a premises vendor include a home builder, premises builder, and premises manager. Examples of a premises vendee include a home buyer, premises buyer, and premises tenant. Examples of a communication service vendor include an Internet service provider, a telephone company, a satellite television company, and a cable television company. Examples of a communication service vendee include a customer of the Internet service provider, a customer of the telephone company, a customer of the satellite television company, and a customer of the cable television company. Premises management services can manage energy of the premises, security of the premises, and/or safety of the premises.

An embodiment of the invention is directed to a system. The system includes a network of premises management devices, a gateway coupled to the network and premises management devices, a server coupled to the gateway by a communication medium and a portal coupled to the communications medium. The portal provides communication with the premises management devices.

According to various embodiments of the invention alone or in various combinations: the communications medium may comprise the Internet; the portal may comprise an Internet portal; and/or the portal may be branded with the name of a vendor of a product associated with the premises. The product may comprise a building, and/or the vendor may comprise a party that leases the premises. The vendor may also or alternatively comprise a property management organization. The server may be included within a network operations center. The logic may comprise, according to various embodiments of the invention, software, hardware, or a combination of software and hardware.

Another embodiment to the invention is directed to a gateway. The gateway includes an interface coupled to a network of premises management devices, logic that receives data from different premises management devices, and an interface coupled to a communications medium that is coupled to a server. The server is coupled to a portal coupled to the communications medium. The portal provides communications with the premises management devices.

According to various embodiments of the invention alone or in various combinations: the communications medium may comprise the Internet; the portal may comprise an Internet to portal; and/or the portal may be branded with the name of a vendor of a product associated with the premises. The product may comprise a building; the vendor may comprise a party that leases the premises; the vendor may comprise a property management organization; and/or the server may be included within a network operations center.

Provided herein is a gateway device for managing a set of two or more local management devices at a location. The gateway device, in some embodiments, comprises a first interface that allows connectivity to a remote network over which the gateway can communicate to remote systems which are remote to the location. In some embodiments, the gateway device comprises a second interface for communication to a local network including a set of local management devices. The gateway device may also comprise a processor, memory. In some embodiments, the gateway device comprises an address of a gateway registry, a serial number of the gateway device, and a key.

In some embodiments, the gateway device comprises logic that, upon initialization of the gateway device, uses the address of the gateway registry to communicate between the gateway device and the gateway registry. In some embodiments, the logic of the gateway device sends, from the gateway device over the remote network, a request to the gateway registry specifying the serial number of the gateway device. In response to the request, in some embodiments, the logic of the gateway device receives in the gateway device, from the gateway registry over the remote network, a response including an address of a gateway server that has an account associated with the gateway device for managing the location associated with the gateway device. In some embodiments, the logic of the gateway device receives, from the gateway registry over the remote network, an identification of the account associated with the gateway device for managing the location associated with the gateway device. The logic of the gateway device, in some embodiments, communicates between the gateway device and the gateway server upon which the account associated with the gateway device is stored using authentication information derived based on the key, and communicates, over the remote network from the gateway device to the gateway server upon which the account associated with the gateway device is stored, the identification of the account that was received from the gateway registry and, in response to the communication of the identification of the account that was received from the gateway registry, receives account information from the gateway server.

The gateway device, in some embodiments, comprises logic that after initialization of the gateway device, uses the account information to manage a set of local management devices connected to a local network located at the location, wherein the gateway device is also located at the location and connected to the local network.

In some embodiments, the account stored on the gateway server includes historical data for the local network. The account stored on the gateway server may include settings for devices associated with the account. The authentication information that may be derived based on the key is derived by applying a hash function to the key. In some embodiments, the serial number of the gateway device comprises the media access control (MAC) address of the gateway device.

In some embodiments, the gateway registry is included on a first server and the gateway server is included on a second server located physically separate from the first server.

In some embodiments, the location may comprise a residence. In other embodiments, the location may comprise a business premises.

In some embodiments, the remote network comprises the Internet.

In some embodiments, the logic comprises a computer. The logic may comprise computer program code stored in a memory on the gateway device. The logic may comprise electronic circuitry included in the gateway device. In some embodiments, the logic comprises electronic circuitry and computer program code in the gateway device.

In some embodiments, the logic for managing the set of local management devices comprises automation logic that initiates actions with respect to the local management devices upon certain conditions. In some embodiments, the automation logic is configured based on account information received from the gateway server. In some embodiments, the logic for managing the set of local management devices takes actions depending on a mode.

Provided herein is a system for networks at a plurality of locations. In some embodiments, the system comprises a plurality of control networks. A control network may include a plurality of management devices at a location and a gateway device, as described herein. The gateway device in a control network may include a first interface for communicating between systems remote from the location, a second interface for communicating between at least one management device at the location, an address of a gateway registry, a serial number of the gateway device, and a key.

The system, in some embodiments, may comprise a gateway registry including serial numbers of gateway devices of the respective control networks, identifications of accounts for the control networks, and the server address of a gateway server upon which the account associated with the control network is stored. The gateway registry may comprise logic that uses the gateway serial number of the gateway device to determine the identification of the account associated with the gateway device, logic that communicates to the gateway device the determined identification of the account associated with the gateway device and the server address of the gateway server upon which the account information is stored.

In some embodiments, the system comprises a gateway server including details of the accounts for the control networks, identifications of the accounts, and keys of gateway devices in the control networks associated with the account. In some embodiments, the server includes logic that authenticates communication from respective gateway devices using the keys stored in the gateway server and authentication information received from respective gateway devices, and logic that provides account information to respective authenticated gateway devices based on identifications of accounts provided by the respective gateway devices.

In some embodiments, the account information provided by logic of the server comprises historical data for the local network. In some embodiments, the account information provided by logic of the server comprises settings for devices associated with the account. In some embodiments, the logic in the gateway server that authenticates applies a hash function to the key stored in the gateway server that is associated with the account. In some embodiments, the authentication information received from the gateway device is derived by applying the hash function to the key stored in the gateway device.

In some embodiments, the system includes a plurality of gateway servers and wherein the gateway registry includes a set of addresses to respective gateway servers and an association between gateway device and respective gateway server. In some embodiments, the gateway registry and the gateway server are comprised by a single computer system. In some embodiments, the gateway registry includes a table having an association between each gateway serial number and corresponding account number and gateway server. In some embodiments, the gateway server includes a table having an association between each gateway account identification and corresponding key.

In some embodiments, the local management devices and the gateway device are coupled by at least one of an RF, Z-wave, a wireless connection, a wired connection, and an IP connection to the local network. In some embodiments, the serial number of the gateway device comprises the media access control (MAC) address of the gateway device. In some embodiments, the gateway registry is included on a first server and the gateway server is included on a second server located physically separate from the first server.

In some embodiments of the system, the location comprises a residence. In some embodiments of the system, the location comprises a business premises. In some embodiments, the remote network comprises the Internet.

Provided herein is a method of operating a gateway device in a control network.

In some embodiments, the method of operating a gateway device in a control, network comprises storing on the gateway device an address of a gateway registry, a serial number of the gateway device, and a key. The method may further comprise using the address of the gateway registry to communicate between the gateway device and the gateway registry, and sending, from the gateway device over the remote network, a request to the gateway registry specifying the serial number of the gateway device.

In response to the request, in some embodiments the method comprises receiving in the gateway device, from the gateway registry over the remote network, a response including an address of a gateway server that has an account associated with the gateway device for managing a set of local management devices connected to a local network located at the location associated with the gateway device. In response to the request, in some embodiments the method comprises receiving in the gateway device, from the gateway registry over the remote network, an identification of the account associated with the gateway device for managing the location associated with the gateway device.

The method may further comprise communicating between the gateway device and the gateway server upon which the account associated with the gateway device is stored using authentication information derived based on the key. In some embodiments, the method comprises communicating, over the remote network from the gateway device to the gateway server upon which the account associated with the gateway device is stored, the identification of the account that was received from the gateway registry. In response to the communication of the identification of the account that was received from the gateway registry, in some embodiments the method comprises receiving account information from the gateway server.

The method may comprise using the account information to manage the set of local management devices connected to the local network located at the location, wherein the gateway device is also located at the location and connected to the local network.

In some embodiments of the method, the authentication information derived based on the key is derived by applying a hash function to the key. In some embodiments of the method the serial number of the gateway device comprises the media access control (MAC) address of the gateway device. In some embodiments of the method, the gateway registry is included on a first server and the gateway server is included on a second server located physically separate from the first server. In some embodiments of the method, the location comprises a residence. In some embodiments of the method, the location comprises a business premises. In some embodiments of the method, the remote network comprises the Internet.

In some embodiments, the method further comprises storing the account identification and the gateway server address in the gateway device.

Provided herein is a method for storing information to operate a gateway device in a control network. In some embodiments, the method comprises storing an identification associated with an account associated with a gateway device, a serial number associated with the gateway device, and a key associated with the gateway device in a location remote from a location of the gateway device. In some embodiments, the method comprises populating a table of a gateway registry with the serial number associated with the gateway device, a gateway server location associated with an account associated with the gateway device, and the identification associated with the gateway device, wherein the serial number, the server location, and the identification are associated with each other in the gateway registry table. In some embodiments, the method comprises populating a table of the gateway server with the identification associated with the gateway device and the key associated with the gateway device, wherein the identification and the key are associated with each other in the gateway server and wherein the identification and key are associated with the account associated with the gateway device in the gateway server.

In some embodiments of the method for storing information to operate a gateway device in a control network, the steps of storing the identification, populating the gateway registry table, and populating the gateway server table may be controlled by a gateway account manager. In some embodiments of the method for storing information to operate a gateway device in a control network, the steps of storing the identification, populating the gateway registry table, and populating the gateway server table may be controlled by a remote management device.

Provided herein is a method for storing information to operate a new gateway device in a control network, wherein the control network has been previously associated with a previous gateway device. The storing of information may be in a location remote from a location of the previous gateway device. The information to operate the new gateway device in the control network may be stored in a table of a gateway registry and in a table of a gateway server.

The method for storing information to operate a new gateway device in a control network may comprise finding an identification associated with an account associated with the previous gateway device stored in the location remote from the location of the previous gateway device. The finding may comprise looking up the identification. The finding may comprise requesting the identification. In some embodiments the location is a master database. In some embodiments, a first serial number associated with the previous gateway device and associated with a server location has been stored in a table of a gateway registry, and a first key associated with the previous gateway device has been stored in a table of a gateway server at the server location. In some embodiments, the identification associated with the account associated with the previous gateway device has been stored in the gateway registry and in the gateway server.

The method for storing information to operate a new gateway device in a control network may further comprise storing a second serial number associated with the new gateway device, and a second key associated with the new gateway device in the location remote from the location of the previous gateway device. In some embodiments, the location is the master database.

The method for storing information to operate a new gateway device in a control network may further comprise populating the table of the gateway registry with the second serial number of the new gateway device by associating the second serial number with the same identification and server location previously associated with a first serial number associated with the previous gateway device, wherein a gateway server location associated with the account associated with the previous gateway device becomes the gateway server location associated with the account associated with the new gateway device, and wherein account identification associated with the account associated with the previous gateway device becomes the gateway server location associated with the account associated with the new gateway device, and wherein the second serial number of the new gateway, the server location, and the identification are associated with each other in the gateway registry table. In some embodiments, the method for storing information to operate a new gateway device in a control network may further comprise populating a table of the gateway server with a second key associated with the new gateway device by associating the second key with the identification in the table previously associated with a first key associated with the previous gateway device, wherein the account and the identification associated with the previous gateway device becomes the account and identification associated with the new gateway device, wherein the identification and the second key are associated with each other and with the account associated with the new gateway device in the table of the gateway server.

In some embodiments, the steps of storing the identification, populating the gateway registry table, and populating the gateway server table may be controlled by a gateway account manager. In some embodiments, the steps of storing the identification, populating the gateway registry table, and populating the gateway server table may be controlled by a remote management device.

Aspects of the systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including programmable logic devices (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects of the systems and methods include: microcontrollers with memory, embedded microprocessors, firmware, software, etc. Furthermore, aspects of the systems and methods may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural network) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

It should be noted that the various functions or processes disclosed herein may be described as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, email, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of components and/or processes under the systems and methods may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

Unless the context clearly requires otherwise, throughout the description and the claims, the words 'comprise,' 'comprising,' and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of 'including, but not limited to.' Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words 'herein,' 'hereunder,' 'above,' 'below,' and words of similar import refer to this application as a whole and not to any particular portions of this application. When the word 'or' is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

The above description of illustrated embodiments of the systems and methods is not intended to be exhaustive or to limit the systems and methods to the precise form disclosed. While specific embodiments of, and examples for, the systems and methods are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the systems and methods, as those skilled in the relevant art will recognize. The teachings of the systems and methods provided herein can be applied to other processing systems and methods, not only for the systems and methods described above.

The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the systems and methods in light of the above detailed description.

In general, the terms used should not be construed to limit the systems and methods to the specific embodiments disclosed in the specification and the claims, but should be construed to include all processing systems that operate under the claims. Accordingly, the systems and methods are not limited by the disclosure.

While certain aspects of the systems and methods may be presented in certain claim forms, the inventors contemplate the various aspects of the systems and methods in any number of claim forms. Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the systems and methods.

What is claimed is:

1. A gateway device for managing a set of local management devices at a location, the gateway device comprising:

a processor coupled to a memory;

a first interface coupled to the processor, wherein the first interface couples via a remote network to remote systems that are remote to the location;

a second interface coupled to the processor, wherein the second interface communicates with a local network including the set of local management devices; and

logic that sends via the remote network a request to a gateway registry, the request specifying a serial number of the gateway device, receives an address of a gateway server that has an account associated with the gateway device and an identification of the account, sends to the gateway server the identification of the account, and manages the set of local management devices using account information received in response to the identification.

2. The gateway device of claim 1, wherein the account includes historical data for the local network.

3. The gateway device of claim 1, wherein the account includes settings for devices associated with the account.

4. The gateway device of claim 1, wherein the logic communicates with the gateway server using authentication information derived based on a key.

5. The gateway device of claim 4, wherein the authentication information is derived by applying a hash function to the key.

6. The gateway device of claim 1, wherein the serial number comprises the media access control (MAC) address of the gateway device.

7. The gateway device of claim 1, wherein the logic comprises a computer readable medium.

8. The gateway device of claim 1, wherein the logic comprises computer program code stored in the memory.

9. The gateway device of claim 1, wherein the logic comprises electronic circuitry coupled to the processor.

10. The gateway device of claim 1, wherein the logic comprises electronic circuitry and computer program code.

11. The gateway device of claim 1, wherein the logic initiates actions with respect to the set of local management devices in response to at least one condition.

12. The gateway device of claim 11, wherein the logic is configured based on account information received from the gateway server.

13. The gateway device of claim 1, wherein the logic initiates an action depending on a mode.

14. The gateway device of claim 1, wherein the gateway registry and the gateway server comprise a single processing device.

15. A system for networks at a plurality of locations, the system comprising:

a plurality of control networks, wherein each control network includes a gateway device and management devices at a location, wherein the gateway device of each control network manages the management devices using account information of an account that corresponds to the gateway device;

a gateway registry including logic that determines an identification of the account using a serial number of the gateway device, and communicates to the gateway device the identification and a server address of a server that includes the account information; and

a server including logic that provides the account information to the gateway device based on the identification received from the gateway device.

16. The system of claim 15, wherein each gateway device includes a first interface that connects to a remote network over which the gateway device communicates to remote systems that are remote to the location.

17. The system of claim 15, wherein each gateway device includes a second interface that communicates with a local network, wherein the local network includes the management devices.

18. The system of claim 15, wherein the gateway registry includes a plurality of serial numbers of a plurality of gateway devices corresponding to the plurality of control networks.

19. The system of claim 15, wherein the gateway registry includes a plurality of identifications of a plurality of accounts corresponding to the plurality of control networks.

20. The system of claim 15, wherein the gateway registry includes the server address of the server that includes the account.

21. The system of claim 15, wherein the server comprises the account information corresponding to a plurality of accounts of the plurality of control networks.

22. The system of claim 15, wherein the server comprises the identification of each account corresponding to each gateway device.

23. The system of claim 15, wherein the server comprises a key of the gateway device.

24. The system of claim 23, wherein the logic of the server authenticates communication from the gateway device using the key and authentication information received from the gateway device.

25. The system of claim 24, wherein the logic of the server applies a hash function to the key.

26. The system of claim 25, wherein the authentication information is derived by applying the hash function to the key stored in the gateway device.

27. The system of claim 15, wherein the account information comprises settings for devices associated with the account.

28. The system of claim 15, including a plurality of servers, wherein the gateway registry includes a set of addresses to respective servers and an association between a respective gateway device and respective server.

29. The system of claim 15, wherein the gateway registry includes a table having an association between each serial number of each gateway and an account number and server corresponding to the gateway.

30. The system of claim 15, wherein the server includes a table having an association between each account identification of each gateway and a corresponding key.

31. The system of claim 15, wherein the serial number of the gateway device comprises the media access control (MAC) address of the gateway device.

32. The system of claim 15, wherein the gateway registry and the server comprise a single processing device.

33. A method of operating a gateway device in a control network, the method comprising:

establishing communication between the gateway device at a location and a gateway registry using an address of the gateway registry;

sending a request to the gateway registry specifying a serial number of the gateway device;

receiving from the gateway registry an address of a gateway server that includes an account comprising account information that corresponds to the gateway device;

receiving an identification of the account;

sending to the gateway server the identification and receiving in response the account information; and

managing a set of local management devices coupled to a local network and located at the location using the account information.

34. The method of claim 33, comprising storing the address of the gateway registry on the gateway device.

35. The method of claim 33, comprising storing the serial number on the gateway device.

36. The method of claim 33, comprising communicating between the gateway device and the gateway server using authentication information derived based on a key.

37. The method of claim 36, comprising storing the key on the gateway device.

38. The method of claim 36, wherein the authentication information is derived based on the key by applying a hash function to the key.

39. The method of claim 33, wherein the serial number of the gateway device comprises the media access control (MAC) address of the gateway device.

40. The method of claim **33**, wherein the gateway registry and the gateway server comprise a single processing device.

41. The method of claim **33**, wherein the gateway registry is included on a first server.

42. The method of claim **41**, wherein the gateway server is included on a second server located physically separate from the first server.

43. The method of claim **33**, wherein the gateway device includes the identification of the account and the address of the gateway server.

* * * * *

EXHIBIT 6

US008638211B2

(12) United States Patent
Cohn et al.

(10) **Patent No.: US 8,638,211 B2**
(45) **Date of Patent: Jan. 28, 2014**

(54) **CONFIGURABLE CONTROLLER AND INTERFACE FOR HOME SMA, PHONE AND MULTIMEDIA**

(75) Inventors: **Alan Wade Cohn**, Austin, TX (US); **Gary Robert Faulkner**, Austin, TX (US); **James A. Johnson**, Austin, TX (US); **James Edward Kitchen**, Austin, TX (US); **David Leon Proft**, Austin, TX (US); **Corey Wayne Quain**, Austin, TX (US)

(73) Assignee: **iControl Networks, Inc.**, Redwood City, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 809 days.

(21) Appl. No.: **12/568,718**

(22) Filed: **Sep. 29, 2009**

(65) **Prior Publication Data**

US 2010/0277300 A1 Nov. 4, 2010

Related U.S. Application Data

(60) Provisional application No. 61/174,366, filed on Apr. 30, 2009.

(51) **Int. Cl.**
G08B 29/00 (2006.01)

(52) **U.S. Cl.**
USPC **340/506**

(58) **Field of Classification Search**
USPC 340/506, 539.1, 539.14, 539.17, 541, 340/3.1; 715/764; 709/219
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,298,253	B2 *	11/2007	Petricoin et al.	340/523
8,086,702	B2 *	12/2011	Baum et al.	709/220
2002/0027504	A1 *	3/2002	Davis et al.	340/540
2003/0062997	A1	4/2003	Naidoo et al.	340/53 I
2004/0117462	A1	6/2004	Bodin et al.	709/220
2004/0117465	A1	6/2004	Bodin et al.	709/222
2005/0216580	A1	9/2005	Raji et al.	709/223
2005/0276389	A1	12/2005	Hinkson et al.	379/37
2006/0051122	A1	3/2006	Kawazu et al.	399/88
2006/0067484	A1	3/2006	Elliot et al.	379/37
2006/0078344	A1	4/2006	Kawazu et al.	399/69
2008/0001734	A1 *	1/2008	Stilp et al.	340/539.22
2009/0066789	A1	3/2009	Baum et al.	348/143

(Continued)

FOREIGN PATENT DOCUMENTS

FR	2 584 217	1/1987
WO	WO 99/34339	7/1999

(Continued)

OTHER PUBLICATIONS

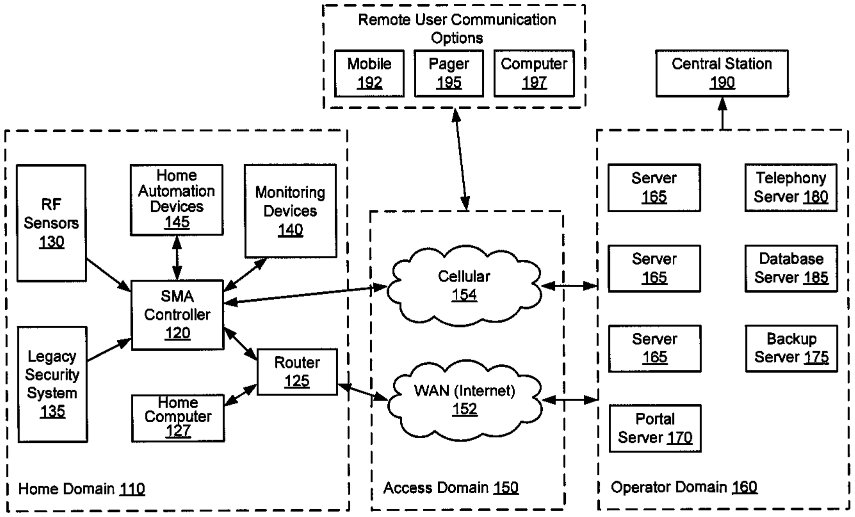
"Control Panel Standard—Features for False Alarm Reduction," The Security Industry Association, © SIA 2009, pp. 1-48.

Primary Examiner — Phung Nguyen
(74) *Attorney, Agent, or Firm* — Gregory & Sawrie LLP

(57) **ABSTRACT**

A single platform for controller functionality for each of security, monitoring and automation, as well as providing a capacity to function as a bidirectional Internet gateway, is provided. Embodiments of the present invention provide such functionality by virtue of a configurable architecture that enables a user to adapt the system for the user's specific needs. Embodiments of the present invention further provide for remote access to the configurable controller, thereby providing for remote monitoring of the state of a dwelling and for remote control of home automation.

33 Claims, 10 Drawing Sheets



Remote User Communication Options
Mobile 192
Pager 195
Computer 197
Central Station 190
RF Sensors 130
Home Automation Devices 145
Monitoring Devices 140
SMA Controller 120
Legacy Security System 135
Router 125
Home Computer 127
Home Domain 110
Cellular 154
WAN (Internet) 152
Access Domain 150
Server 165
Server 165
Server 165
Telephony Server 180
Database Server 185
Backup Server 175
Portal Server 170
Operator Domain 160

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0070436	A1 *	3/2009	Dawes et al.	709/219
2009/0070477	A1	3/2009	Baum et al.	709/231
2009/0070681	A1	3/2009	Dawes et al.	715/736
2009/0070682	A1	3/2009	Dawes et al.	715/736
2009/0070692	A1 *	3/2009	Dawes et al.	715/764
2009/0074184	A1	3/2009	Baum et al.	380/205
2009/0077167	A1	3/2009	Baum et al.	709/203
2009/0077622	A1	3/2009	Baum et al.	726/1
2009/0077623	A1	3/2009	Baum et al.	726/1
2009/0077624	A1	3/2009	Baum et al.	726/1
2009/0134998	A1	5/2009	Baum et al.	340/539.1
2009/0138600	A1	5/2009	Baum et al.	709/226
2009/0138958	A1	5/2009	Baum et al.	726/12
2009/0165114	A1	6/2009	Baum et al.	726/12

FOREIGN PATENT DOCUMENTS

WO	WO 2004/098127	11/2004
WO	WO 2005/091218	9/2005
WO	WO 2009/006670	1/2009

* cited by examiner

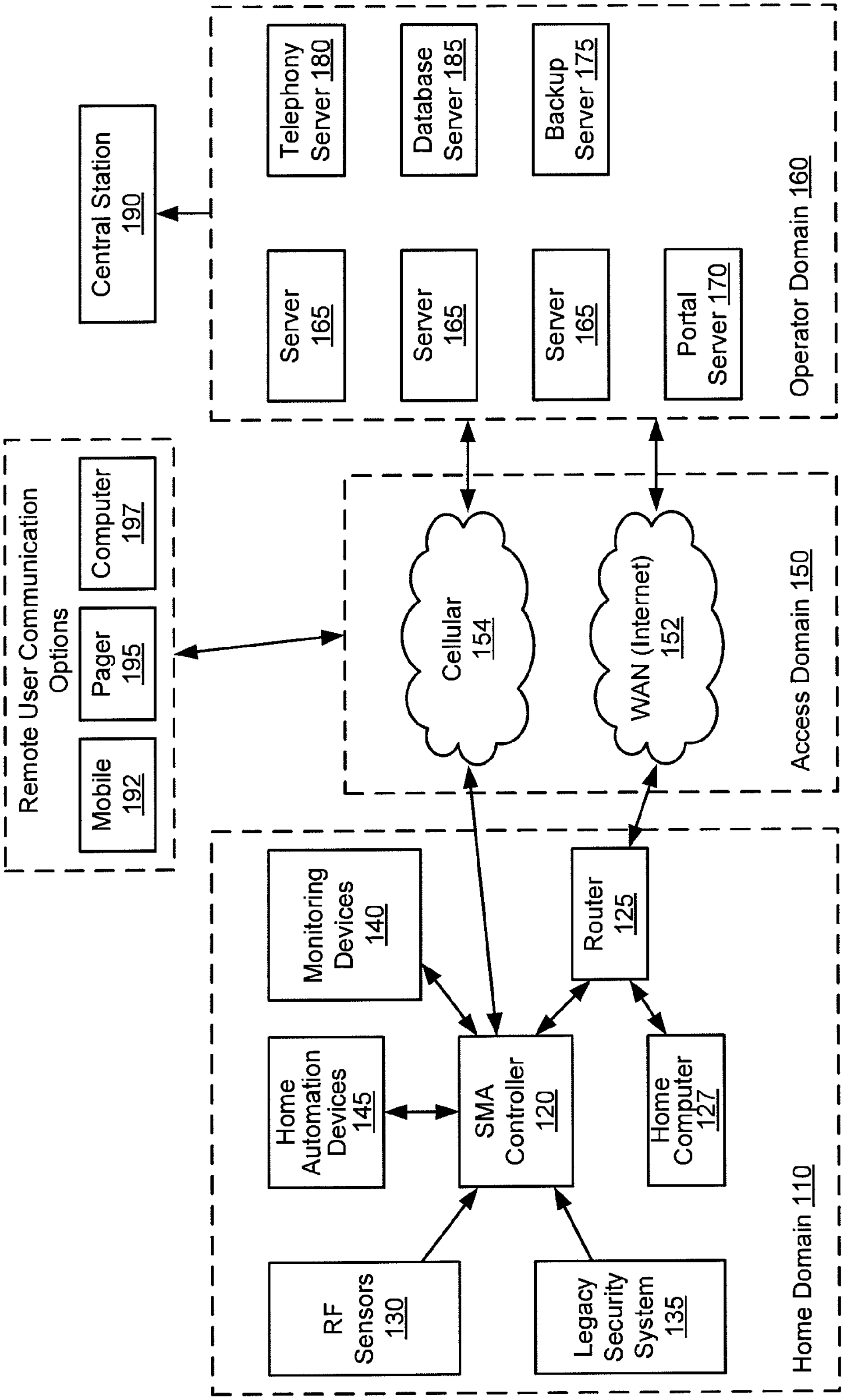

Central Station 190
Telephony Server 180
Database Server 185
Backup Server 175
Server 165
Server 165
Server 165
Portal Server 170
Operator Domain 160
Remote User Communication Options
Mobile 192
Pager 195
Computer 197
Cellular 154
WAN (Internet) 152
Access Domain 150
Monitoring Devices 140
Router 125
Home Automation Devices 145
SMA Controller 120
Home Computer 127
RF Sensors 130
Legacy Security System 135
Home Domain 110

Figure 1

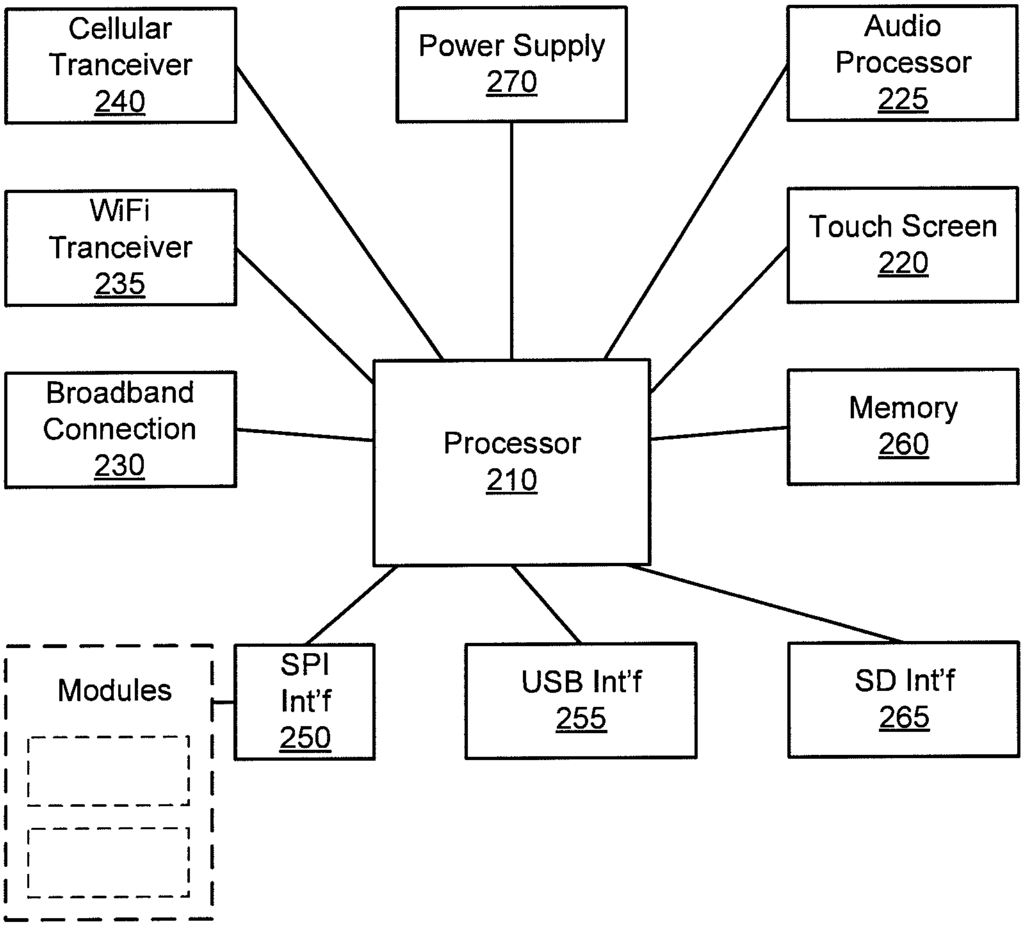

Cellular
Tranceiver
240
Power Supply
270
Audio
Processor
225
WiFi
Tranceiver
235
Touch Screen
220
Broadband
Connection
230
Processor
210
Memory
260
Modules
SPI
Int'f
250
USB Int'f
255
SD Int'f
265

Figure 2

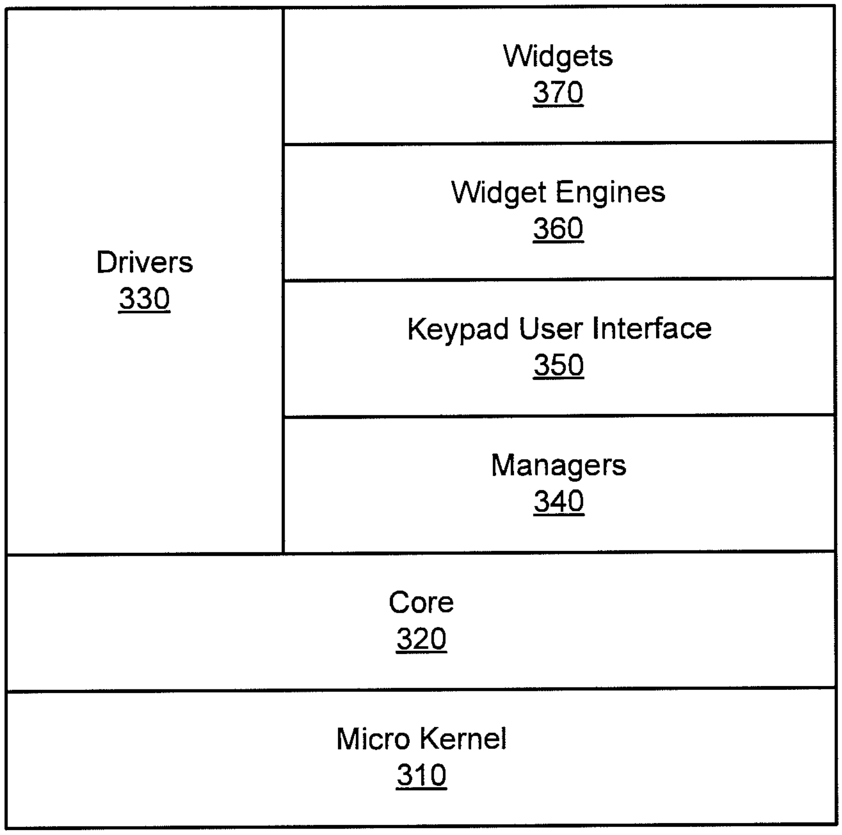

Widgets
370
Widget Engines
360
Drivers
330
Keypad User Interface
350
Managers
340
Core
320
Micro Kernel
310

Figure 3

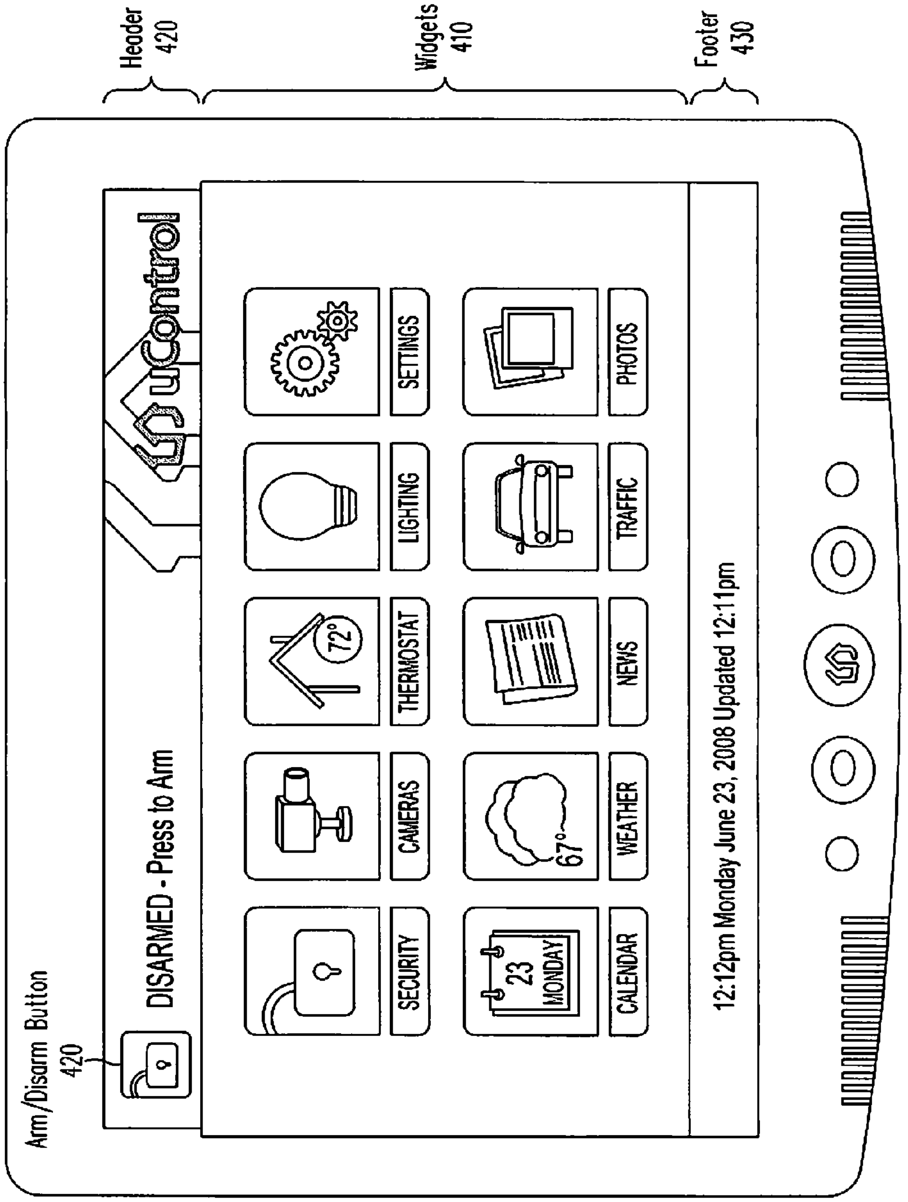

Header
420
Widgets
410
Footer
430
Arm/Disarm Button
420
DISARMED - Press to Arm
uControl
SECURITY
CAMERAS
THERMOSTAT
72°
LIGHTING
SETTINGS
23
MONDAY
CALENDAR
67°
WEATHER
NEWS
TRAFFIC
PHOTOS
12:12pm Monday June 23, 2008 Updated 12:11pm

Figure 4

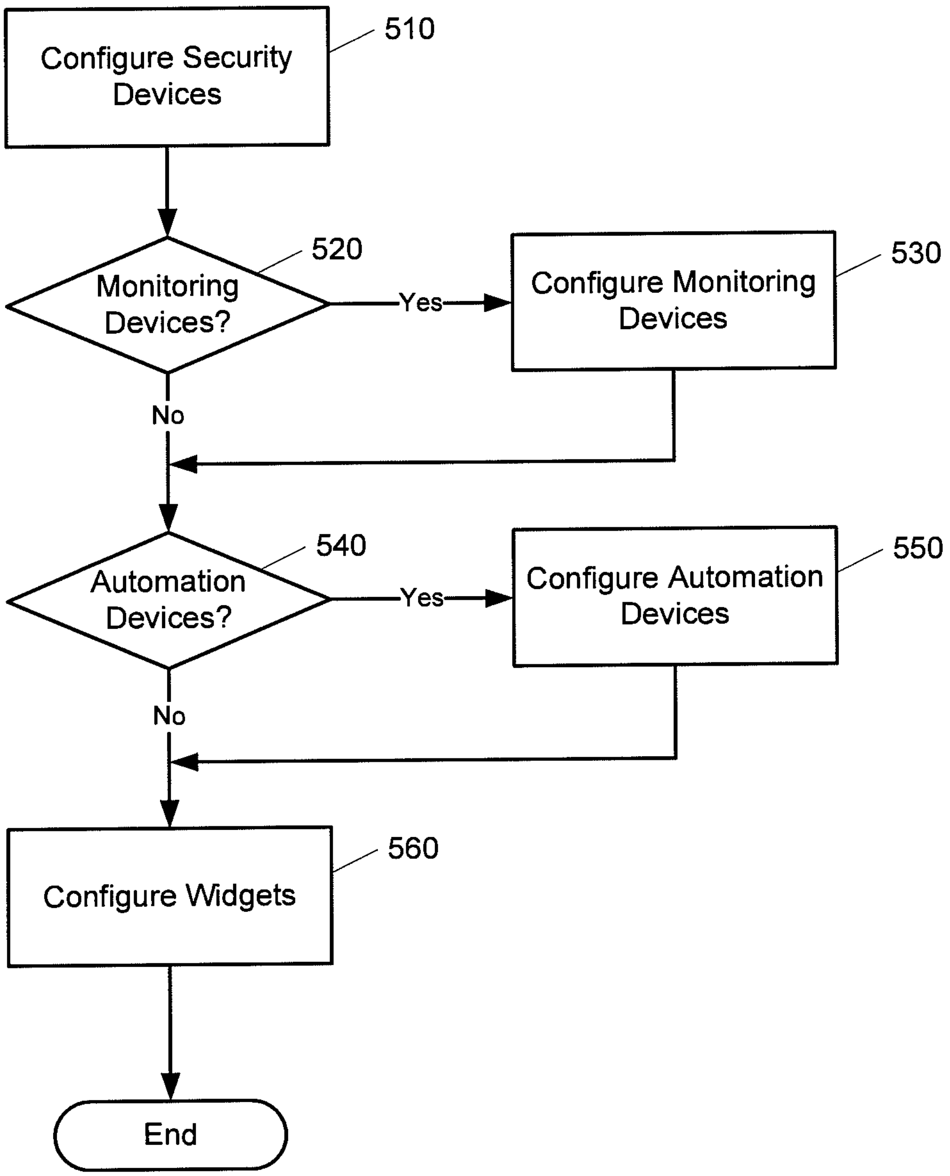
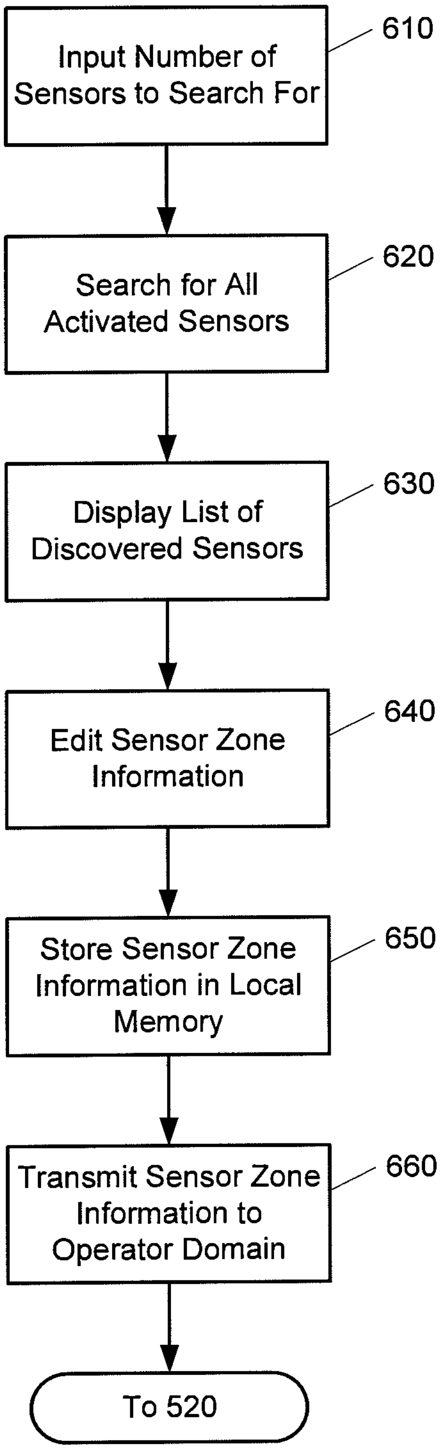

Configure Security Devices
510
Monitoring Devices?
520
Yes
Configure Monitoring Devices
530
No
Automation Devices?
540
Yes
Configure Automation Devices
550
No
Configure Widgets
560
End

Figure 5



Input Number of Sensors to Search For
610
Search for All Activated Sensors
620
Display List of Discovered Sensors
630
Edit Sensor Zone Information
640
Store Sensor Zone Information in Local Memory
650
Transmit Sensor Zone Information to Operator Domain
660
To 520

Figure 6

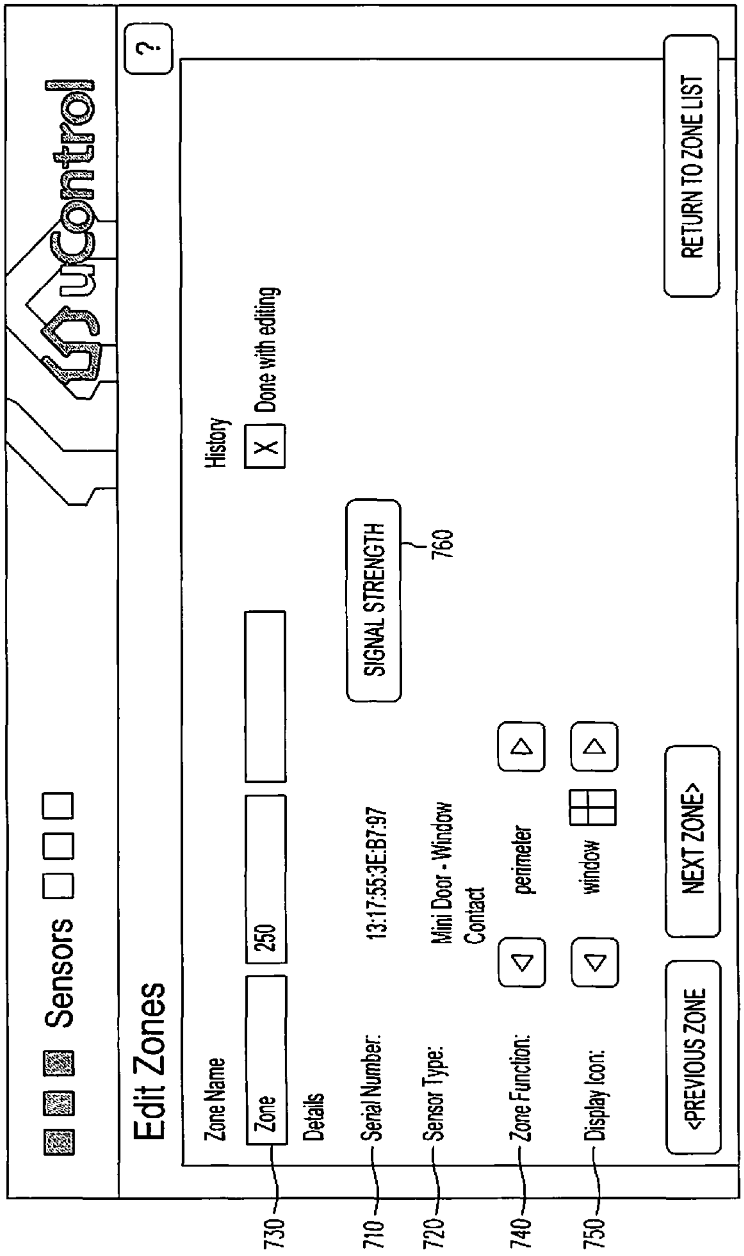

Sensors
uControl
?
Edit Zones
Zone Name
Zone
250
Details
Serial Number:
13:17:55:3E:B7:97
Sensor Type:
Mini Door - Window Contact
Zone Function:
perimeter
Display Icon:
window
History
X
Done with editing
SIGNAL STRENGTH
760
<PREVIOUS ZONE
NEXT ZONE>
RETURN TO ZONE LIST
730
710
720
740
750

Figure 7

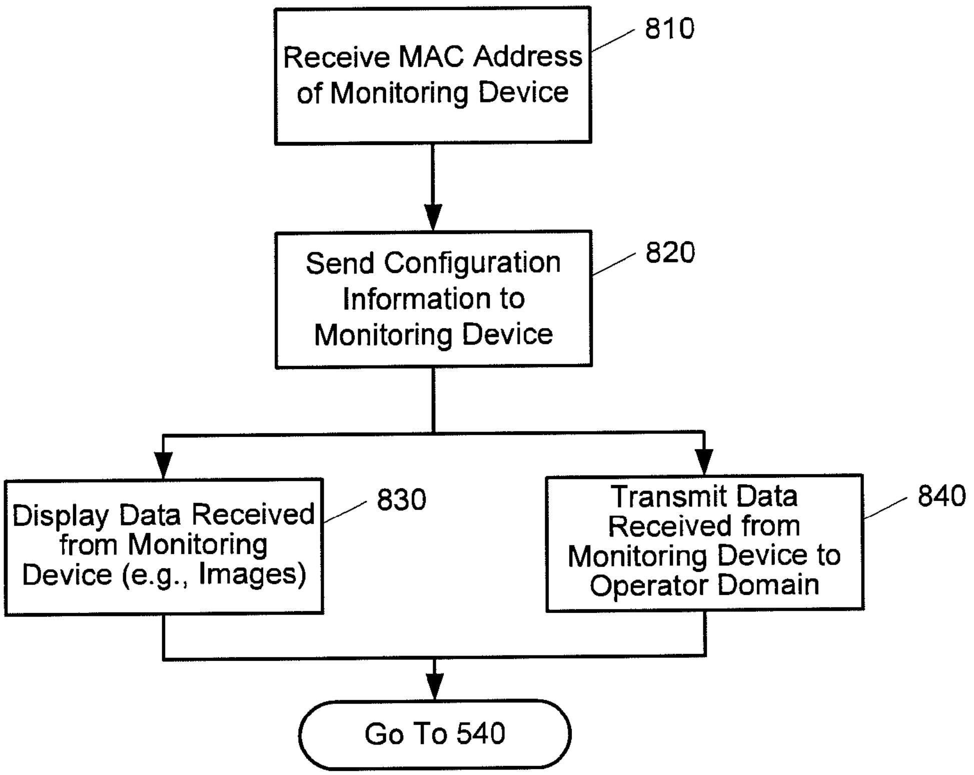

Receive MAC Address of Monitoring Device
810
Send Configuration Information to Monitoring Device
820
Display Data Received from Monitoring Device (e.g., Images)
830
Transmit Data Received from Monitoring Device to Operator Domain
840
Go To 540

Figure 8

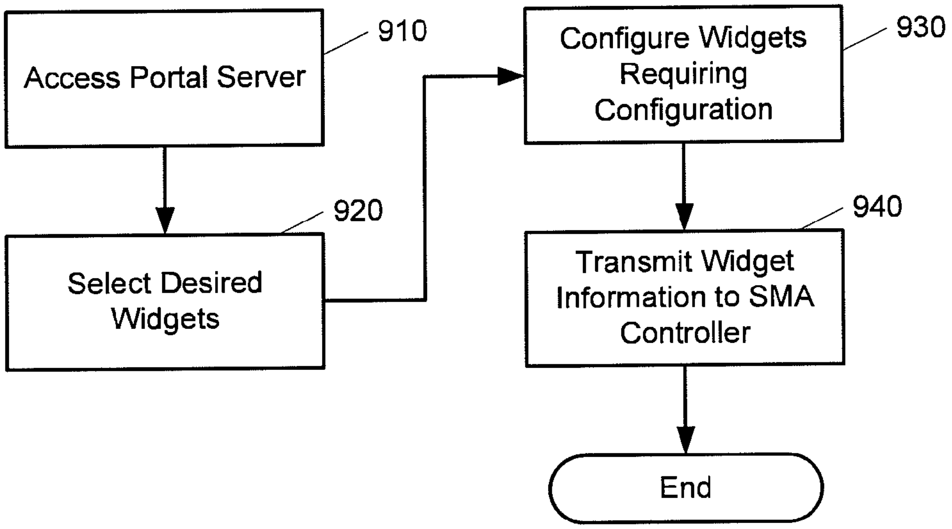

Access Portal Server
910
Select Desired Widgets
920
Configure Widgets Requiring Configuration
930
Transmit Widget Information to SMA Controller
940
End

Figure 9

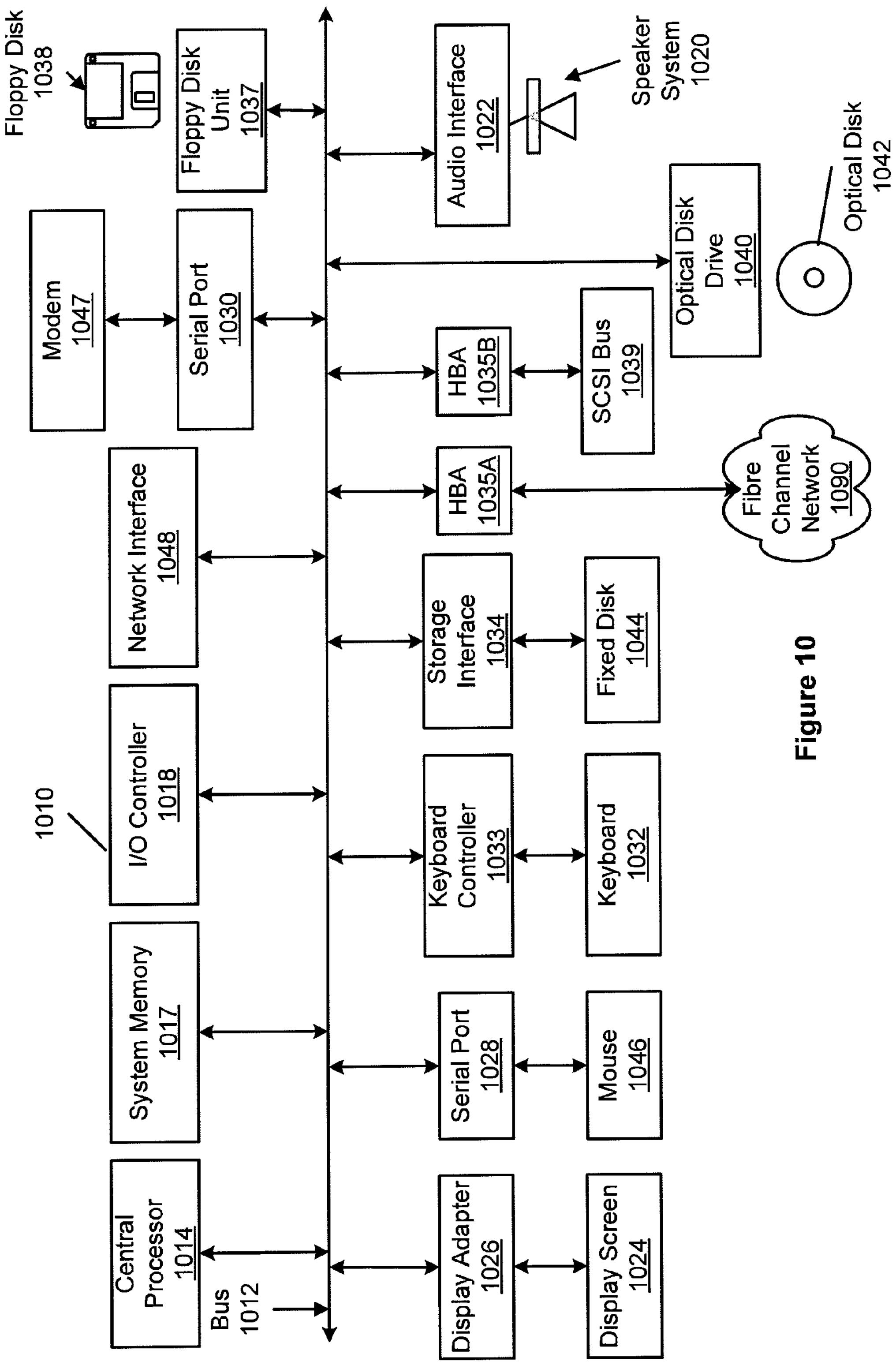
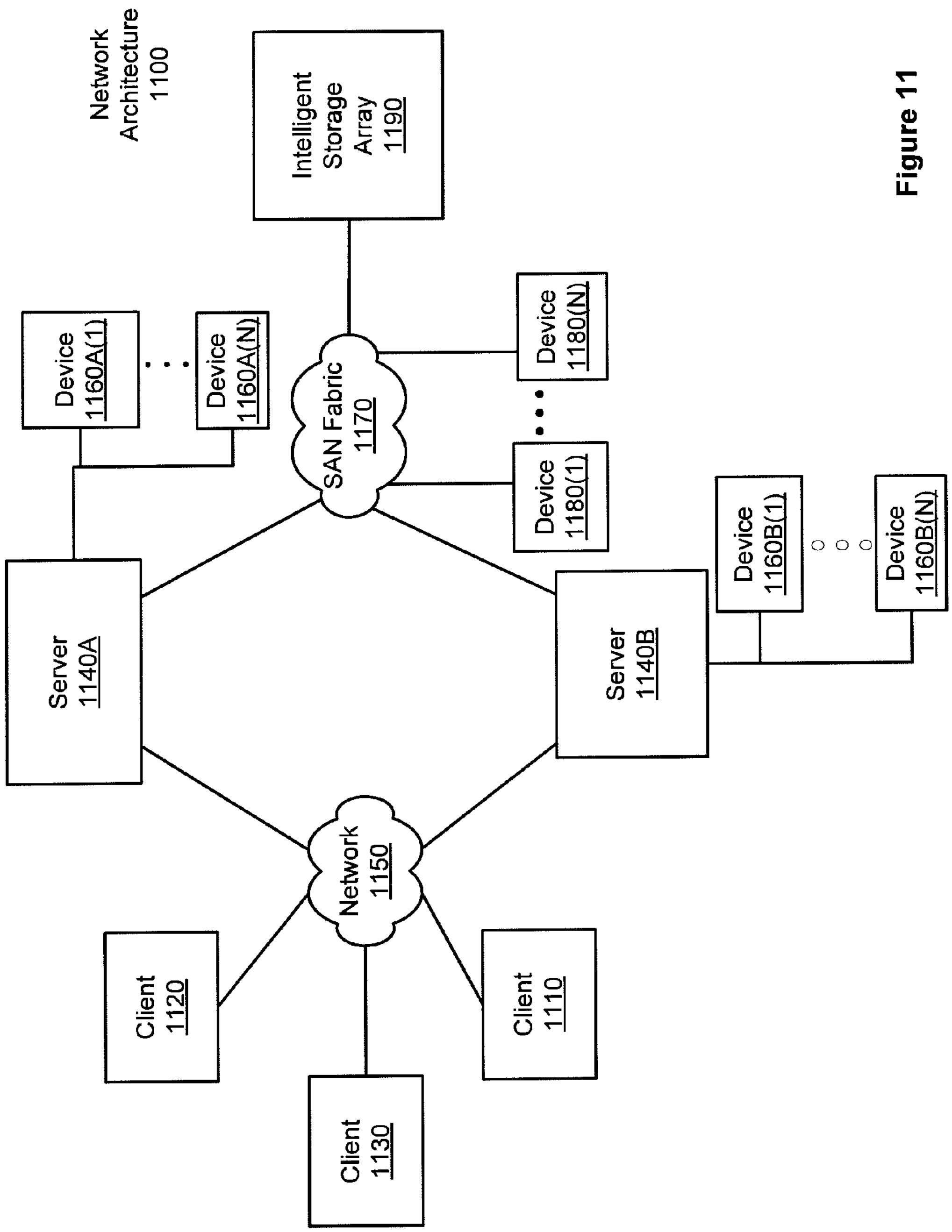

Floppy Disk 1038
Floppy Disk Unit 1037
Modem 1047
Serial Port 1030
Network Interface 1048
1010
I/O Controller 1018
System Memory 1017
Central Processor 1014
Bus 1012
Audio Interface 1022
Speaker System 1020
Optical Disk Drive 1040
Optical Disk 1042
HBA 1035B
SCSI Bus 1039
HBA 1035A
Fibre Channel Network 1090
Storage Interface 1034
Fixed Disk 1044
Keyboard Controller 1033
Keyboard 1032
Serial Port 1028
Mouse 1046
Display Adapter 1026
Display Screen 1024

Figure 10



Network Architecture 1100
Intelligent Storage Array 1190
Device 1160A(1)
Device 1160A(N)
SAN Fabric 1170
Device 1180(N)
Device 1180(1)
Device 1160B(1)
Device 1160B(N)
Server 1140A
Server 1140B
Network 1150
Client 1120
Client 1130
Client 1110

Figure 11

CONFIGURABLE CONTROLLER AND INTERFACE FOR HOME SMA, PHONE AND MULTIMEDIA

CROSS REFERENCE TO RELATED APPLICATIONS

This invention claims priority from Provisional Patent Application Ser. No. 61/174,366, entitled "REMOTE SECURITY STATION," filed Apr. 30, 2009, and naming Alan Wade Cohn as inventor. This provisional patent application is incorporated herein by reference in its entirety and for all purposes.

FIELD OF THE INVENTION

Embodiments of the present invention relate generally to the field of home security, monitoring and automation, and specifically to a user-configurable controller for security, monitoring and automation.

BACKGROUND OF THE INVENTION

Residential electronics and control standards provide an opportunity for a variety of options for securing, monitoring, and automating residences. Wireless protocols for transmission of security information permit placement of a multitude of security sensors throughout a residence without a need for running wires back to a central control panel. Inexpensive wireless cameras also allow for placement of cameras throughout a residence to enable easy monitoring of the residence. A variety of home automation control protocols have also been developed to allow for centralized remote control of lights, appliances, and environmental apparatuses (e.g., thermostats). Traditionally, each of these security, monitoring and automation protocols require separate programming, control and monitoring stations. To the extent that home automation and monitoring systems have been coupled to home security systems, such coupling has involved including the automation and monitoring systems as slaves to the existing home security system. This limits the flexibility and versatility of the automation and monitoring systems and ties such systems to proprietary architectures.

A security system alerts occupants of a dwelling and emergency authorities of a violation of premises secured by the system. A typical security system includes a controller connected by wireless or wired connections to sensors deployed at various locations throughout the secured dwelling. In a home, sensors are usually deployed in doorways, windows, and other points of entry. Motion sensors can also be placed strategically within the home to detect unauthorized movement, while smoke and heat sensors can detect the presence of fire.

A home monitoring system provides an ability to monitor a status of a home so that a user can be made aware of any monitored state changes. For example, when a sensor is tripped, real-time alerts and associated data such as video or photo clips can be sent to the user (e.g., to a network-connected computer or to a mobile device).

A home automation system enables automation and remote control of lifestyle conveniences such as lighting, heating, cooling, and appliances. Typically these various lifestyle conveniences are coupled to a controller via wireless or wired communications protocols. A central device is then used to program the various lifestyle conveniences.

Rather than having multiple devices to control each of the security, monitoring and automation environments, it is desirable to have a centralized controller capable of operating in each environment, thereby reducing the equipment needed in a dwelling. It is further desirable for such a controller to function as a gateway for external network access so that a user can control or monitor devices in locations remote from the dwelling. It is further desirable for such a combined controller and gateway to provide configurable flexibility in how devices in the various environments are monitored and controlled.

SUMMARY OF THE INVENTION

Embodiments of the present invention provide a single platform that provides controller functionality for each of security, monitoring and automation, as well as providing a capacity to function as a bidirectional Internet gateway. Embodiments of the present invention provide such functionality by virtue of a configurable architecture that enables a user to adapt the system for the user's specific needs. Embodiments of the present invention further provide for remote access to the configurable controller, thereby providing for remote monitoring of the state of a dwelling and for remote control of home automation.

One embodiment of the present invention includes memory for storing configuration information for security sensors, monitoring devices and automation devices, communication interfaces for communicating with one or more of these devices and a remote server, and a processor for interpreting event signals from the security sensors and transmitting data associated with the event signals to the remote server. One aspect of this embodiment of the present invention provides for the interpretation of the event signals to be performed in accordance with the configuration information of the associated security sensor. A further aspect of this embodiment of the present invention provides for the transmitted event-related data to conform to the associated configuration information.

A further aspect of the above embodiment of the present invention provides for a display device coupled to the processor for displaying event-related data. Another aspect of the above embodiment of the present invention provides for an input device coupled to the processor for inputting configuration information associated with a sensor device, a monitoring device or an automation device. Further aspects of the present invention provides for receiving and transmitting the configuration information from and to the remote server.

An additional aspect of the above embodiment of the present invention provides for generating configuration information for a monitoring device and providing that configuration information to the monitoring device. Another aspect of the above embodiment of the present invention provides for receiving data from a monitoring device and transmitting data from the monitoring device to the remote server. A further aspect of the above embodiment of the present invention provides for receiving data from a monitoring device and displaying that data on a display coupled to the processor. Another aspect of the above embodiment of the present invention provides for communicating control information to a monitoring device.

An additional aspect of the above embodiment of the present invention provides for communication of control information to an automation device. Such control information can be provided by an input device coupled to the processor or by the remote server.

Another aspect of the above embodiment of the present invention provides for display and execution of widget application programs. The widget application programs can be selected from a set of available widget application programs on the remote server. The remote server can then distribute the selected widget application programs to the device.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

FIG. **1** is a simplified block diagram illustrating an architecture including a set of logical domains and functional entities within which embodiments of the present invention interact.

FIG. **2** is a simplified block diagram illustrating a hardware architecture of an SMA controller, according to one embodiment of the present invention.

FIG. **3** is a simplified block diagram illustrating a logical stacking of an SMA controller's firmware architecture, usable with embodiments of the present invention.

FIG. **4** is an illustration of an example user interface for an SMA controller **120**, according to an embodiment of the present invention.

FIG. **5** is a simplified flow diagram illustrating steps performed in a configuration process of an SMA controller, in accord with embodiments of the present invention.

FIG. **6** is a simplified flow diagram illustrating steps performed in configuring security sensors (e.g., **510**), in accord with embodiments of the present invention.

FIG. **7** is an illustration of a display that can be provided by embodiments of the present invention to permit editing of sensor information (e.g., sensor zone information).

FIG. **8** is a simplified flow diagram illustrating steps performed to configure a home domain monitoring device, in accord with embodiments of the present invention.

FIG. **9** is a simplified flow diagram illustrating steps performed in selecting widgets for use by an SMA controller, in accord with embodiments of the present invention.

FIG. **10** depicts a block diagram of a computer system **1010** suitable for implementing aspects of the present invention (e.g., servers **165**, portal server **170**, backup server **175**, telephony server **180**, and database server **185**).

FIG. **11** is a block diagram depicting a network architecture **1100** in which client systems **1110**, **1120** and **1130**, as well as storage servers **1140**A and **1140**B (any of which can be implemented using computer system **1010**), are coupled to a network **1150**.

DETAILED DESCRIPTION

Embodiments of the present invention provide a single platform that provides controller functionality for each of security, monitoring and automation, as well as providing a capacity to function as a bidirectional Internet gateway. Embodiments of the present invention provide such functionality by virtue of a configurable architecture that enables a user to adapt the system for the user's specific needs. Embodiments of the present invention further provide for remote access to the configurable controller, thereby providing for remote monitoring of the state of a dwelling and for remote control of home automation.

Architectural Overview

Embodiments of the configurable security, monitoring and automation (SMA) controller of the present invention provide not only for communicating with and interpreting signals from sensors and devices within a dwelling, but also for accessing and monitoring those sensors and devices from locations remote to the dwelling. Embodiments of the SMA controller provide such capability through linkages to external servers via access networks such as the Internet, provider network, or a cellular network. The external servers provide a portal environment through which a user can, for example, monitor the state of sensors coupled to the SMA controller in real-time, configure the controller, and provide controlling information to the SMA controller. The servers can further automatically provide information to a user via remote devices such as mobile phones, computers, and pagers. The servers further provide a connection to a traditional security central station, which can then contact authorities in the event of an alarm condition being detected by the SMA controller in the dwelling.

FIG. **1** is a simplified block diagram illustrating an architecture including a set of logical domains and functional entities within which embodiments of the present invention interact. A home domain **110** includes an embodiment of the SMA controller **120**. The home domain is coupled via an access domain **150** to an operator domain **160** that includes various servers. The servers are in turn coupled to a central station **190** and to various remote user communication options.

The home domain refers to a collection of security, monitoring and automation entities within a dwelling or other location having SMA devices. SMA controller **120** is a device that provides an end-user SMA interface to the various SMA entities within home domain **110**. SMA controller **120** further acts as a gateway interface between home domain **110** and operator domain **160**. SMA gateway **120** provides such gateway access to operator domain **160** via a network router **125**. Network router **125** can be coupled to SMA controller **120** and to home network devices such as home computer **127** via either hard wired or wireless connections. A network router **125** coupled to a broadband modem (e.g., a cable modem or DSL modem) serves as one link to networks in access domain **150**.

SMA devices within home domain **110** can include a variety of RF or wireless sensors **130** whose signals are received and interpreted by SMA gateway **120**. RF sensors **130** can include, for example, door or window sensors, motion detectors, smoke detectors, glass break detectors, inertial detectors, water detectors, carbon dioxide detectors, and key fob devices. SMA gateway **120** can be configured to react to a change in state of any of these detectors. In addition to acting and reacting to changes in state of RF sensors **130**, SMA controller **120** also can be coupled to a legacy security system **135**. SMA controller **120** controls the legacy security system by interpreting signals from sensors coupled to the legacy security system and reacting in a user-configured manner. SMA gateway **120**, for example, will provide alarm or sensor state information from legacy security system **135** to servers in operator domain **160** that may ultimately inform central station **190** to take appropriate action.

SMA gateway **120** can also be coupled to one or more monitoring devices **140**. Monitoring devices **140** can include, for example, still and video cameras that provide images that are viewable on a screen of SMA gateway **120** or a remotely connected device. Monitoring devices **140** can be coupled to SMA gateway **120** either wirelessly (e.g., WiFi via router **125**) or other connections.

Home automation devices **145** can also be coupled to and controlled by SMA gateway **120**. SMA gateway **120** can be configured to interact with a variety of home automation protocols, such as, for example, Z-Wave and ZigBee.

Embodiments of SMA controller **120** can be used to configure and control home security devices (e.g., **130** and **135**), monitoring devices **140** and automation devices **145**, either directly or by providing a gateway to remote control via servers in operator domain **160**. SMA controller **120** communicates with servers residing in operator domain **160** via networks in access domain **150**. Broadband communication can be provided by coupling SMA controller **120** with a network router **125**, which in turn is coupled to a wide area network **152**, such as a provider network or the Internet, via an appropriate broadband modem. The router can be coupled to the wide area network through cable broadband, DSL, and the like. Wide area network **152**, in turn, is coupled to servers in operator domain **160** via an appropriate series of routers and firewalls (not shown). SMA controller **120** can include additional mechanisms to provide a communication with the operator domain. For example, SMA controller **120** can be configured with a cellular network transceiver that permits communication with a cellular network **154**. In turn, cellular network **154** can provide access via routers and firewalls to servers in operator domain **160**. Embodiments of SMA controller **120** are not limited to providing gateway functionality via cellular and dwelling-based routers and modems. For example, SMA gateway **120** can be configured with other network protocol controllers such as WiMAX satellite-based broadband, direct telephone coupling, and the like.

Operator domain **160** refers to a logical collection of SMA servers and other operator systems in an operator's network that provide end-user interfaces, such as portals accessible to subscribers of the SMA service, that can configure, manage and control SMA elements within home domain **110**. Servers in operator domain **160** can be maintained by a provider (operator) of subscriber-based services for SMA operations. Examples of providers include cable providers, telecommunications providers, and the like. A production server architecture in operator domain **160** can support SMA systems in millions of home domains **110**.

Individual server architectures can be of a variety of types, and in one embodiment, the server architecture is a tiered Java2 Enterprise Edition (J2EE) service oriented architecture. Such a tiered service oriented architecture can include an interface tier, a service tier, and a data access logic tier. The interface tier can provide entry points from outside the server processes, including, for example, browser web applications, mobile web applications, web services, HTML, XHTML, SOAP, and the like. A service tier can provide a variety of selectable functionality passed along by the operator to the end user. Service tiers can relate to end user subscription levels offered by the operator (e.g., payment tiers corresponding to "gold" level service, "silver" level service and "bronze" level service). Finally the data access logic tier provides access to various sources of data including database servers.

FIG. **1** illustrates an example set of servers that can be provided in operator domain **160**. Servers **165** can support all non-alarm and alarm events, heartbeat, and command traffic between the various servers and SMA controllers **120**. Servers **165** can also manage end-user electronic mail and SMS notification, as well as integration with provider billing, provisioning, inventory, tech support systems, and the like.

A portal server **170** can provide various user interface applications, including, for example, a subscriber portal, a mobile portal, and a management portal. A subscriber portal is an end-user accessible application that permits an end-user to access a corresponding SMA controller remotely via standard web-based applications. Using such a subscriber portal provides access to the same SMA functions that an interface directly coupled to the SMA controller would provide, plus additional functions such as alert and contact management, historical data, widget and camera management, account management, and the like. A mobile portal can provide all or part of the access available to an end-user via the subscriber portal. A mobile portal can be limited, however, to capabilities of an accessing mobile device (e.g., touch screen or non-touch screen cellular phones). A management portal provides an operator representative access to support and manage SMA controllers in home domains **110** and corresponding user accounts via a web-based application. The management portal can provide tiers of management support so that levels of access to user information can be restricted based on authorization of a particular employee.

Telephony server **180** can process and send information related to alarm events received from SMA controllers **120** to alarm receivers at central monitoring station **190**. A server **165** that processes the alarm event makes a request to telephony server **180** to dial the central station's receiver and send corresponding contact information. Telephony server **180** can communicate with a plurality of central stations **190**. Server **165** can determine a correct central station to contact based upon user account settings associated with the transmitting SMA controller. Thus, alarms can be routed to different central stations based upon user accounts. Further, accounts can be transferred from one central station to another by modifying user account information. Telephony server **180** can communicate with alarm receivers at central station **190** using, for example, a security industry standard contact identification protocol (e.g., dual-tone multi-frequency [DTMF]) and broadband protocols.

A backup server **175** can be provided to guarantee that an alarm path is available in an event that one or more servers **165** become unavailable or inaccessible. A backup server **175** can be co-located to the physical location of servers **165** to address scenarios in which one or more of the servers fail. Alternatively, a backup server **175** can be placed in a location remote from servers **165** in order to address situations in which a network failure or a power failure causes one or more of servers **165** to become unavailable. SMA controllers **120** can be configured to transmit alarm events to a backup server **175** if the SMA controller cannot successfully send such events to servers **165**.

A database server **185** provides storage of all configuration and user information accessible to other servers within operator domain **160**. Selection of a type of database provided by database server **185** can be dependent upon a variety of criteria, including, for example, scalability and availability of data. One embodiment of the present invention uses database services provided by an ORACLE database.

A server **165** in operator domain **160** provides a variety of functionality. Logically, a server **165** can be divided into the following functional modules: a broadband communication module, a cellular communication module, a notification module, a telephony communication module, and an integration module.

The broadband communication module manages broadband connections and message traffic from a plurality of SMA controllers **110** coupled to server **165**. Embodiments of the present invention provide for the broadband channel to be a primary communication channel between an SMA controller **120** and servers **165**. The broadband communication module handles a variety of communication, including, for example, all non-alarm and alarm events, broadband heartbeat, and command of traffic between server **165** and SMA controller **120** over the broadband channel. Embodiments of the present invention provide for an always-on persistent TCP socket connection to be maintained between each SMA controller and server **165**. A variety of protocols can be used for communications between server **165** and SMA controller **120** (e.g., XML over TCP, and the like). Such communication can be secured using standard transport layer security (TLS) technologies. Through the use of an always-on socket connection, servers **165** can provide near real-time communication between the server and an SMA controller **120**. For example, if a user has a subscriber portal active and a zone is tripped within home domain **110**, a zone fault will be reflected in near real-time on the subscriber portal user interface.

The cellular communication module manages cellular connections and message traffic from SMA controllers **120** to a server **165**. Embodiments of the present invention use the cellular channel as a backup communication channel to the broadband channel. Thus, if a broadband channel becomes unavailable, communication between an SMA controller and a server switches to the cellular channel. At this time, the cellular communication module on the server handles all non-alarm and alarm events, and command traffic from an SMA controller. When a broadband channel is active, heartbeat messages can be sent periodically on the cellular channel in order to monitor the cellular channel. When a cellular protocol communication stack is being used, a TCP socket connection can be established between the SMA controller and server to ensure reliable message delivery for critical messages (e.g., alarm events and commands). Once critical messages have been exchanged, the TCP connection can be shut down thereby reducing cellular communication costs. As with broadband communication, XMPP can be the messaging protocol used for such communications. Similarly, such communication can be secured using TLS and SASL authentication protocols. Non-critical messages between an SMA controller and a server can be sent using UDP. A compressed binary protocol can be used as a messaging protocol for such communications in order to minimize cellular costs for such message traffic. Such messages can be secured using an encryption algorithm, such as the tiny encryption algorithm (TEA). Cellular communication can be established over two network segments: the GSM service provider's network that provides a path between an SMA controller and a cellular access point, and a VPN tunnel between the access point and an operator domain data center.

A notification module of server **165** determines if and how a user should be notified of events generated by their corresponding SMA controller **120**. A user can specify who to notify of particular events or event types and how to notify the user (e.g., telephone call, electronic mail, text message, page, and the like), and this information is stored by a database server **185**. When events such as alarm or non-alarm events are received by a server **165**, those events can be past asynchronously to the notification module, which determines if, who and how to send those notifications based upon the user's configuration.

The telephony communication module provides communication between a server **165** and telephony server **180**. When a server **165** receives and performs initial processing of alarm events, the telephony communication module forwards those events to a telephony server **180** which in turn communicates with a central station **190**, as discussed above.

The integration module provides infrastructure and interfaces to integrate a server **165** with operator business systems, such as, for example, billing, provisioning, inventory, tech support, and the like. An integration module can provide a web services interface for upstream integration that operator business systems can call to perform operations like creating and updating accounts and querying information stored in a database served by database server **185**. An integration module can also provide an event-driven framework for downstream integration to inform operator business systems of events within the SMA system.

SMA Controller Architecture

FIG. **2** is a simplified block diagram illustrating a hardware architecture of an SMA controller, according to one embodiment of the present invention. A processor **210** is coupled to a plurality of communications transceivers, interface modules, memory modules, and user interface modules. Processor **210**, executing firmware discussed below, performs various tasks related to interpretation of alarm and non-alarm signals received by SMA controller **120**, interpreting reactions to those signals in light of configuration information either received from a server (e.g., server **165**) or entered into an interface provided by SMA controller **120** (e.g., a touch screen **220**). Embodiments of the present invention can use a variety of processors, for example, an ARM core processor such as a FREESCALE i.MX35 multimedia applications processor.

SMA controller **120** can provide for user input and display via a touch screen **220** coupled to processor **210**. Processor **210** can also provide audio feedback to a user via use of an audio processor **225**. Audio processor **225** can, in turn, be coupled to a speaker that provides sound in home domain **110**. SMA controller **120** can be configured to provide a variety of sounds for different events detected by sensors associated with the SMA controller. Such sounds can be configured by a user so as to distinguish between alarm and non-alarm events.

As discussed above, an SMA controller **120** can communicate with a server **165** using different network access means. Processor **210** can provide broadband access to a router (e.g., router **125**) via an Ethernet broadband connection PHY **130** or via a WiFi transceiver **235**. The router can then be coupled to or be incorporated within an appropriate broadband modem. Cellular network connectivity can be provided by a cellular transceiver **240** that is coupled to processor **210**. SMA controller **120** can be configured with a set of rules that govern when processor **210** will switch between a broadband connection and a cellular connection to operator domain **160**.

In order to communicate with the various sensors and devices within home domain **110**, processor **210** can be coupled to one or more transceiver modules via, for example, a serial peripheral interface such as a SPI bus **250**. Such transceiver modules permit communication with sensors of a variety of protocols in a configurable manner. Embodiments of the present invention can use a Bosch transceiver to communicate with a variety of RF sensors **130**. Similarly, home automation transceivers that communicate using Z-Wave or ZigBee protocols can be coupled to processor **210** via SPI **250**. If SMA controller **120** is coupled to a legacy security system **135**, then a module permitting coupling to the legacy security system can be coupled to processor **210** via SPI **250**. Other protocols can be provided for via such plug-in modules including, for example, digital enhanced cordless telecommunication devices (DECT). In this manner, an SMA controller **120** can be configured to provide for control of a variety of devices and protocols known both today and in the future. In addition, processor **210** can be coupled to other types of devices (e.g., transceivers or computers) via a universal serial bus (USB) interface **255**.

In order to locally store configuration information for SMA controller **120**, a memory **260** is coupled to processor **210**. Additional memory can be coupled to processor **210** via, for example, a secure digital interface **265**. A power supply **270** is also coupled to processor **210** and to other devices within SMA controller **120** via, for example, a power management controller module.

SMA controller **120** is configured to be a customer premises equipment device that works in conjunction with server counterparts in operator domain **160** in order to perform functions required for security monitoring and automation. Embodiments of SMA controller **120** provide a touch screen interface (e.g., **220**) into all the SMA features. Via the various modules coupled to processor **210**, the SMA controller bridges the sensor network, the control network, and security panel network to broadband and cellular networks. SMA controller **120** further uses the protocols discussed above to carry the alarm and activity events to servers in the operator domain for processing. These connections also carry configuration information, provisioning commands, management and reporting information, security authentication, and any real-time media such as video or audio.

FIG. **3** is a simplified block diagram illustrating a logical stacking of an SMA controller's firmware architecture, usable with embodiments of the present invention. Since SMA controller **120** provides security functionality for home domain **110**, the SMA controller should be a highly available system. High availability suggests that the SMA controller be ready to serve an end-user at all times, both when a user is interacting with the SMA controller through a user interface and when alarms and other non-critical system events occur, regardless of whether a system component has failed. In order to provide such high availability, SMA controller **120** runs a micro-kernel operating system **310**. An example of a micro-kernel operating system usable by embodiments of the present invention is a QNX real-time operating system. Under such a micro-kernel operating system, drivers, applications, protocol stacks and file systems run outside the operating system kernel in memory-protected user space. Such a micro-kernel operating system can provide fault resilience through features such as critical process monitoring and adaptive partitioning. As a result, components can fail, including low-level drivers, and automatically restart without affecting other components or the kernel and without requiring a reboot of the system. A critical process monitoring feature can automatically restart failed components because those components function in the user space. An adaptive partitioning feature of the micro kernel operating system provides guarantees of CPU resources for designated components, thereby preventing a component from consuming all CPU resources to the detriment of other system components.

A core layer **320** of the firmware architecture provides service/event library and client API library components. A client API library can register managers and drivers to handle events and to tell other managers or drivers to perform some action. The service/event library maintains lists of listeners for events that each manager or driver detects and distributes according to one of the lists.

Driver layer **330** interacts with hardware peripherals of SMA controller **120**. For example, drivers can be provided for touch screen **220**, broadband connection **230**, WiFi transceiver **235**, cellular transceiver **240**, USB interface **255**, SD interface **265**, audio processor **225**, and the various modules coupled to processor **210** via SPI interface **250**. Manager layer **340** provides business and control logic used by the other layers. Managers can be provided for alarm activities, security protocols, keypad functionality, communications functionality, audio functionality, and the like.

Keypad user interface layer **350** drives the touch screen user interface of SMA controller **120**. An example of the touch screen user interface consists of a header and a footer, widget icons and underlying widget user interfaces. Keypad user interface layer **350** drives these user interface elements by providing, for example, management of what the system Arm/Disarm interface button says and battery charge information, widget icon placement in the user face area between the header and footer, and interacting with widget engine layer **360** to display underlying widget user interface when a widget icon is selected.

In embodiments of the present invention, typical SMA controller functions are represented in the touch screen user interface as widgets (or active icons). Widgets provide access to the various security monitoring and automation control functions of SMA controller **120** as well as providing support for multi-media functionality through widgets that provide, for example, news, sports, weather and digital picture frame functionality. A main user interface screen can provide a set of icons, each of which represents a widget. Selection of a widget icon can then launch the widget. Widget engine layer **360** includes, for example, widget engines for native, HTML and FLASH-based widgets. Widget engines are responsible for displaying particular widgets on the screen. For example, if a widget is developed in HTML, selection of such a widget will cause the HTML widget engine to display the selected widget or touch screen **220**. Information related to the various widgets is provided in widget layer **370**.

FIG. **4** is an illustration of an example user interface for an SMA controller **120**, according to an embodiment of the present invention. The illustrated user interface provides a set of widget icons **410** that provide access to functionality of SMA controller **120**. As illustrated, widgets are provided to access security functionality, camera images, thermostat control, lighting control, and other settings of the SMA controller. Additional widgets are provided to access network-based information such as weather, news, traffic, and digital picture frame functionality. A header **420** provides access to an Arm/Disarm button **425** that allows for arming the security system or disarming it. Additional information can be provided in the header, such as, for example, network status messages. A footer **430** can provide additional status information such as time and date, as displayed.

A user can select widgets corresponding to desired functionality. Embodiments of the present invention provide for access to widgets via portal server **170**. A provider of operator domain **160** can determine functionality accessible to users, either for all users or based upon tiers of users (e.g., subscription levels associated with payment levels). A user can then select from the set of accessible widgets and the selected widgets will be distributed and displayed on the user interface of SMA controller **120**. Configurability of SMA controller **120** is also driven by user determined actions and reactions to sensor stimulus.

SMA Controller Configurability

In accord with embodiments of the present invention, SMA controller **120** can be configured by a user in order to provide desired functionality in home domain **110**. In addition to the hardware configurable options discussed above (e.g., modules coupled to SPI interface **250**), SMA controller **120** provides for additional configuration through the use of software and/or firmware. For example, SMA controller **120** can be configured to receive signals from a variety of security sensors (e.g., RF sensors **130**) and to associate those sensors with the physical environment of home domain **110**. In addition, SMA controller **120** can be configured to receive still and video information from one or more cameras, provide a variety of programs and utilities to a user, and is configurable to communicate with a variety of home automation devices.

FIG. **5** is a simplified flow diagram illustrating steps performed in a configuration process of an SMA controller, in accord with embodiments of the present invention. Embodiments of an SMA controller will typically be configured with security sensor information, either from RF sensors **130** or from a legacy security system **135**. Therefore, an SMA controller will be configured to access and interpret information related to those security sensors (**510**).

A determination can then be made as to whether or not a user is including security cameras in home domain **110** (**520**). If cameras are included in the home domain, then a series of steps related to camera configuration is performed (**530**). Similarly, a determination can be made as to whether or not home automation devices are to be controlled by the SMA controller (**540**). If so, then a series of steps can be performed to configure the SMA controller to access those home automation devices (**550**).

A user can then perform steps necessary to configuring widgets accessible via the SMA controller (**560**). As discussed above, the user may access a portal server (e.g., **170**) to select and configure those widgets that are desirable to be accessed at SMA controller **120**. Once these configuration steps are performed, the SMA controller can be made available to perform tasks related to securing, monitoring, and providing automation control to home domain **110**.

SMA controller **120** can be configured to receive and interpret signals from a variety of security sensors. Such sensors can include, for example, door/window sensors that can detect opening and closing of a door or window, motion detectors that can detect movement in an area of interest, smoke detectors, glass break detectors, inertia detectors, and key fobs. In order to usefully interpret signals from such detectors, embodiments of SMA controller **120** can search for signals from such sensors and be configured with information related to the location and tasks of those sensors.

FIG. **6** is a simplified flow diagram illustrating steps performed in configuring security sensors (e.g., **510**), in accord with embodiments of the present invention. A user of a security system incorporating SMA controller **120** (e.g., an owner or resident of home domain **110**) can decide, based upon the needs within the home domain, the types and number of security sensors needed to secure the home domain. SMA controller **120**, via a touch screen input device, for example, can be told how many such sensors to search for (**610**). The SMA controller can then search for all activated sensors providing a linking message to the SMA controller (**620**). Such a linking message can provide sensor information including, for example, a unique identification number for the sensor and sensor type information. A touch screen interface for SMA controller **120** can then provide to the user a display indicating information related to all sensors found during the search (**630**).

Once presented with information related to all the located sensors, a user can then edit that information to provide specifics as to physical, or zone, location of the sensor within the home domain and other characteristics related to the zone of the sensor (**640**). For example, a touch screen display **220** coupled to SMA controller **120** can provide a list of all located sensors from which the user can select a specific sensor to define or edit information related to that sensor. The information related to the sensors and zones is then stored in a local memory of the SMA controller **120** (e.g., memory **260**) (**650**). The SMA controller can also transmit the sensor zone information to be stored in a server in operator domain **160** via an available broadband connection (**660**).

FIG. **7** is an illustration of a display that can be provided by embodiments of the present invention to permit editing of sensor information (e.g., sensor zone information). As illustrated, the display can provide information such as the unique identifier of the sensor (serial number **710**) and the sensor type (sensor type **720**). As indicated above, unique identifier and sensor type information is provided by the sensor during the search and location process. Through a display such as that illustrated in FIG. **7**, a user can define additional zone characteristics related to the sensor. For example, a user can define or select a zone name **730** to associate with the sensor. Such a zone name can be entered by a user through the use of a touch screen-based keyboard or selected from a list of common names displayed on the touch screen.

A zone function **740** can also be provided to be associated with the sensor. A zone function determines behavior of the zone and is dependent on the zone type. For example, a door/window sensor can function as an entry/exit zone or as a perimeter zone. Each zone type can have one or more configurable zone functions. For example, a motion detector can have a zone function of interior follower, a smoke/heat detector can have a zone function of 24-hour fire monitoring, a glass break detector can have a zone function of a perimeter zone, and an inertia detector can have an entry/exit zone function or a perimeter zone function.

Selection of a zone function definition alters how the security system acts and reacts to signals received from a sensor in that zone. The following table illustrates examples of zone functions and their associated action/reaction definitions.

TABLE 1

Zone Function	Definition
Entry/Exit	Allow exiting the home domain when the system is arming and will begin an entry delay when opened if the system is armed. Zone can be bypassed and can have specific tones assigned for open and close events.
Perimeter	Generate an alarm immediately if tripped while the system is armed. Can be bypassed and can have specific tones assigned for open and close events.
Interior Follower	Protect the internal spaces of the home domain and trigger an immediate alarm if the system is armed in away mode. Zone is not armed when the system is in armed stay mode. Can be bypassed and can have specific activity/non activity tones assigned.
24-Hour Fire	Generate an immediate fire alarm if triggered. Zone cannot be bypassed.
24-Hour Monitor	Generate notifications in the home and will beep the keypad but will not sound the full alarm. Can be bypassed.
24-Hour Environmental	Generates notifications, beeps keypads, and sounds the siren to let people within the home domain know to evacuate the premises. Cannot be bypassed.
24-Hour Inform	Will never generate an alarm, even if the system is armed. Upon triggering of the sensor will make the configured sound and send events to the operator domain. Can be bypassed.

By defining such zones, a user can control how the security functions of SMA controller **120** react to various sensor triggers.

A user can also configure a display icon **750** associated with the sensor zone. In many cases, the available icons will be limited to one type of icon that graphically relates to the sensor type. But, for example, with a door/window sensor, icons can be made available that illustrate a door or a window as appropriate. FIG. **7** further illustrates a signal strength button **760** that, when selected, can illustrate strength of the signal between the wireless hub located within SMA controller **120** and the associated sensor.

The sensor zone information entered through the use of a display such as that illustrated in FIG. **7**, can be stored in local data tables that are stored in memory **260** of SMA controller **120** (**650**). In addition, sensor zone information can also be transmitted via access domain **150** to servers in operator domain **160** for storage (e.g., database server **185**) (**660**). By storing the sensor zone information in servers in the operator domain, the information is available to a user accessing a portal server **170**. A user could then edit the sensor zone information through use of the portal rather than the SMA controller interface. Further, sensor zone information stored on database server **185** is retained even if an SMA controller suffers from an event that makes the SMA controller unusable. In such an event, a new SMA controller can be installed in home domain **110** and the information stored in operator domain **160** can be provided to the new SMA controller. This eliminates a need to manually reconfigure the new SMA controller with all sensor information.

FIG. **8** is a simplified flow diagram illustrating steps performed to configure a home domain monitoring device, in accord with embodiments of the present invention. As discussed above, SMA controller **120** can communicate with home domain monitoring devices **140**, such as cameras and audio monitors. For example, a wireless camera can be activated and can communicate with SMA controller **120** via a router **125**. During configuration, the SMA controller can detect the presence of a camera by receiving an MAC address of the camera from the router (**810**). The SMA controller can then configure the camera to communicate wirelessly with the router and the SMA controller (**820**). The SMA controller can pass a variety of information to the camera during a configuration phase, including, for example, an administrative user name and password, camera name, camera description, time zone, current time, language, user session name and password for list of users allowed to access the camera, network settings such as IP address and name servers, protocol settings, motion detection settings, and desired camera image settings such as resolution and video adjustments. In addition, the camera can provide information to the SMA controller for storage, such as, for example, device type, manufacturer, model number, and other control information.

Once the SMA controller and camera are configured, then images generated by the camera can be displayed on a display device associated with SMA controller **120** (**830**) or can be communicated to a portal server in operator domain **160** via a network in access domain **150** for display on a computer or mobile devices communicating with the portal server (**840**). SMA controller **120** can also store information related to the camera, such as, for example, a camera name, location of the camera, and relationship of the camera with a defined sensor zone. Embodiments of the present invention can provide both still and video images either on the SMA controller display or a portal display. An SMA controller can be configured to communicate with more than one monitoring device.

SMA controller **120** also has a capability of providing access to a variety of functionality through the use of widget programs. FIG. **4**, discussed above, illustrates an example of a home screen display of SMA controller **120**, showing a set of icons having associated widget programs (**410**). Some of the widgets provide for SMA controller functionality, such as, for example, security access, camera monitoring, and setting modification. Additionally, widgets can be provided to access SMA controller automation functionality such as thermostat control and lighting control. In addition, an SMA controller can provide display of user-selectable widgets (e.g., calendar, weather, news, traffic, and photos).

FIG. **9** is a simplified flow diagram illustrating steps performed in selecting widgets for use by an SMA controller, in accord with embodiments of the present invention. A user can select those user selectable widget programs that are desired by accessing a portal server **170** (**910**). The user can view those widget programs that are available to the user and select those that the user wishes to install on the SMA controller (**920**). A user can also configure how the widget icons are displayed on the home screen (e.g., position of each icon) as well as provide any individual widget configuration information (e.g., zip code information for weather and traffic widgets) (**930**). Depending upon the purpose of a widget, a user may have a variety of options in configuring that widget.

By making widgets available on a portal server in the operator domain, the operator can control the nature and types of widgets available to a user. For example, an operator can define a series of option tiers for their users, with each tier having increasing numbers of available widgets or different type of widget functionality. Further, by making the widgets available through the portal, an operator can control the quality of the available widgets and ensuring that widgets will not affect the operability of SMA controller under the operator's control.

Once selected, code related to the widgets and widget setup information is transferred from servers in operator domain **160** to the associated SMA controller **120** in home domain **110** (**940**). That code information is stored in SMA controller **120**, for example, in memory **260**.

SMA controller **120** can also be configured to provide home automation functionality. As discussed above, a variety of hardware modules can be coupled to the SMA controller, allowing the SMA controller to communicate using protocols associated with those modules. In addition to the hardware configurability, SMA controller **120** is configured to communicate with a variety of devices selected to be controlled by the SMA controller. In a manner similar to that discussed above with regard to configuration of security sensors, SMA controller **120** is configured to detect available automated devices and display information regarding those devices. A user can then edit information about those devices and behavior of those devices through, for example, a touch screen interface coupled to SMA controller **120**. In addition, a user can provide automation commands via accessing portal server **170** to modify those settings, or take immediate control of an automated device. Similarly, a user can take immediate control of automated devices from the touch screen of the SMA controller (e.g., through use of widgets such as "lights" and "thermostat," illustrated in FIG. **4**). Configuration information related to the automated devices can be stored in a memory of SMA controller **120** or in a server located in operator domain **160**.

In this manner, embodiments of the present invention provide configurable control over a variety of SMA devices in the home domain using a single controller. A variety of different device protocols can be provided for through the use of plug-in modules. Further flexibility is provided through configurable set up and control of security and automation devices. Additional functionality is provided through the use of user-selectable and user-configurable widgets.

An Example Computing and Network Environment

As shown above, the present invention can be implemented using a variety of computer systems and networks. An example of one such computing and network environment is described below with reference to FIGS. **10** and **11**.

FIG. **10** depicts a block diagram of a computer system **1010** suitable for implementing aspects of the present invention (e.g., servers **165**, portal server **170**, backup server **175**, telephony server **180**, and database server **185**). Computer system **1010** includes a bus **1012** which interconnects major subsystems of computer system **1010**, such as a central processor **1014**, a system memory **1017** (typically RAM, but which may also include ROM, flash RAM, or the like), an input/output controller **1018**, an external audio device, such as a speaker system **1020** via an audio output interface **1022**, an external device, such as a display screen **1024** via display adapter **1026**, serial ports **1028** and **1030**, a keyboard **1032** (interfaced with a keyboard controller **1033**), a storage interface **1034**, a floppy disk drive **1037** operative to receive a floppy disk **1038**, a host bus adapter (HBA) interface card **1035**A operative to connect with a Fibre Channel network **1090**, a host bus adapter (HBA) interface card **1035**B operative to connect to a SCSI bus **1039**, and an optical disk drive **1040** operative to receive an optical disk **1042**. Also included are a mouse **1046** (or other point-and-click device, coupled to bus **1012** via serial port **1028**), a modem **1047** (coupled to bus **1012** via serial port **1030**), and a network interface **1048** (coupled directly to bus **1012**).

Bus **1012** allows data communication between central processor **1014** and system memory **1017**, which may include read-only memory (ROM) or flash memory (neither shown), and random access memory (RAM) (not shown), as previously noted. The RAM is generally the main memory into which the operating system and application programs are loaded. The ROM or flash memory can contain, among other code, the Basic Input-Output system (BIOS) which controls basic hardware operation such as the interaction with peripheral components. Applications resident with computer system **1010** are generally stored on and accessed via a computer-readable medium, such as a hard disk drive (e.g., fixed disk **1044**), an optical drive (e.g., optical drive **1040**), a floppy disk unit **1037**, or other storage medium. Additionally, applications can be in the form of electronic signals modulated in accordance with the application and data communication technology when accessed via network modem **1047** or interface **1048**.

Storage interface **1034**, as with the other storage interfaces of computer system **1010**, can connect to a standard computer-readable medium for storage and/or retrieval of information, such as a fixed disk drive **1044**. Fixed disk drive **1044** may be a part of computer system **1010** or may be separate and accessed through other interface systems. Modem **1047** may provide a direct connection to a remote server via a telephone link or to the Internet via an internet service provider (ISP). Network interface **1048** may provide a direct connection to a remote server via a direct network link to the Internet via a POP (point of presence). Network interface **1048** may provide such connection using wireless techniques, including digital cellular telephone connection, Cellular Digital Packet Data (CDPD) connection, digital satellite data connection or the like.

Many other devices or subsystems (not shown) may be connected in a similar manner (e.g., document scanners, digital cameras and so on). Conversely, all of the devices shown in FIG. **10** need not be present to practice the present invention. The devices and subsystems can be interconnected in different ways from that shown in FIG. **10**. The operation of a computer system such as that shown in FIG. **10** is readily known in the art and is not discussed in detail in this application. Code to implement the present invention can be stored in computer-readable storage media such as one or more of system memory **1017**, fixed disk **1044**, optical disk **1042**, or floppy disk **1038**. The operating system provided on computer system **1010** may be MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, Linux®, or another known operating system.

Moreover, regarding the signals described herein, those skilled in the art will recognize that a signal can be directly transmitted from a first block to a second block, or a signal can be modified (e.g., amplified, attenuated, delayed, latched, buffered, inverted, filtered, or otherwise modified) between the blocks. Although the signals of the above described embodiment are characterized as transmitted from one block to the next, other embodiments of the present invention may include modified signals in place of such directly transmitted signals as long as the informational and/or functional aspect of the signal is transmitted between blocks. To some extent, a signal input at a second block can be conceptualized as a second signal derived from a first signal output from a first block due to physical limitations of the circuitry involved (e.g., there will inevitably be some attenuation and delay). Therefore, as used herein, a second signal derived from a first signal includes the first signal or any modifications to the first signal, whether due to circuit limitations or due to passage through other circuit elements which do not change the informational and/or final functional aspect of the first signal.

FIG. **11** is a block diagram depicting a network architecture **1100** in which client systems **1110**, **1120** and **1130**, as well as storage servers **1140**A and **1140**B (any of which can be implemented using computer system **1010**), are coupled to a network **1150**. Storage server **1140**A is further depicted as having storage devices **1160**A(**1**)-(N) directly attached, and storage server **1140**B is depicted with storage devices **1160**B (**1**)-(N) directly attached. Storage servers **1140**A and **1140**B are also connected to a SAN fabric **1170**, although connection to a storage area network is not required for operation of the invention. SAN fabric **1170** supports access to storage devices **1180**(**1**)-(N) by storage servers **1140**A and **1140**B, and so by client systems **1110**, **1120** and **1130** via network **1150**. Intelligent storage array **1190** is also shown as an example of a specific storage device accessible via SAN fabric **1170**.

With reference to computer system **1010**, modem **1047**, network interface **1048** or some other method can be used to provide connectivity from each of client computer systems **1110**, **1120** and **1130** to network **1150**. Client systems **1110**, **1120** and **1130** are able to access information on storage server **1140**A or **1140**B using, for example, a web browser or other client software (not shown). Such a client allows client systems **1110**, **1120** and **1130** to access data hosted by storage server **1140**A or **1140**B or one of storage devices **1160**A(**1**)-(N), **1160**B(**1**)-(N), **1180**(**1**)-(N) or intelligent storage array **1190**. FIG. **11** depicts the use of a network such as the Internet for exchanging data, but the present invention is not limited to the Internet or any particular network-based environment.

Other Embodiments

The present invention is well adapted to attain the advantages mentioned as well as others inherent therein. While the present invention has been depicted, described, and is defined by reference to particular embodiments of the invention, such references do not imply a limitation on the invention, and no such limitation is to be inferred. The invention is capable of considerable modification, alteration, and equivalents in form and function, as will occur to those ordinarily skilled in the pertinent arts. The depicted and described embodiments are examples only, and are not exhaustive of the scope of the invention.

The foregoing describes embodiments including components contained within other components (e.g., the various elements shown as components of computer system **1010**). Such architectures are merely examples, and, in fact, many other architectures can be implemented which achieve the same functionality. In an abstract but still definite sense, any arrangement of components to achieve the same functionality is effectively "associated" such that the desired functionality is achieved. Hence, any two components herein combined to achieve a particular functionality can be seen as "associated with" each other such that the desired functionality is achieved, irrespective of architectures or intermediate components. Likewise, any two components so associated can also be viewed as being "operably connected," or "operably coupled," to each other to achieve the desired functionality.

The foregoing detailed description has set forth various embodiments of the present invention via the use of block diagrams, flowcharts, and examples. It will be understood by those within the art that each block diagram component, flowchart step, operation and/or component illustrated by the use of examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or any combination thereof For example, specific electronic components can be employed in an application specific integrated circuit or similar or related circuitry for implementing the functions associated with one or more of the described functional blocks.

The present invention has been described in the context of fully functional computer systems; however, those skilled in the art will appreciate that the present invention is capable of being distributed as a program product in a variety of forms, and that the present invention applies equally regardless of the particular type of computer-readable media used to actually carry out the distribution. Examples of computer-readable media include computer-readable storage media, as well as media storage and distribution systems developed in the future.

The above-discussed embodiments can be implemented by software modules that perform one or more tasks associated with the embodiments. The software modules discussed herein may include script, batch, or other executable files. The software modules may be stored on a machine-readable or computer-readable storage media such as magnetic floppy disks, hard disks, semiconductor memory (e.g., RAM, ROM, and flash-type media), optical discs (e.g., CD-ROMs, CD-Rs, and DVDs), or other types of memory modules. A storage device used for storing firmware or hardware modules in accordance with an embodiment of the invention can also include a semiconductor-based memory, which may be permanently, removably or remotely coupled to a microprocessor/memory system. Thus, the modules can be stored within a computer system memory to configure the computer system to perform the functions of the module. Other new and various types of computer-readable storage media may be used to store the modules discussed herein.

The above description is intended to be illustrative of the invention and should not be taken to be limiting. Other embodiments within the scope of the present invention are possible. Those skilled in the art will readily implement the steps necessary to provide the structures and the methods disclosed herein, and will understand that the process parameters and sequence of steps are given by way of example only and can be varied to achieve the desired structure as well as modifications that are within the scope of the invention. Variations and modifications of the embodiments disclosed herein can be made based on the description set forth herein, without departing from the scope of the invention.

Consequently, the invention is intended to be limited only by the scope of the appended claims, giving full cognizance to equivalents in all respects.

What is claimed is:

1. A device comprising:

a memory storing configuration information for one or more security sensors, configuration information for one or more monitoring devices, and configuration information for one or more automation devices;

a first communication interface for communication with the one or more security sensors;

a second communication interface for communication with a remote server; and

a processor, coupled to the memory and the first and second communication interfaces, configured to interpret an event signal received via the first communication interface from a first security sensor of the one or more security sensors, wherein said interpreting is performed in accord with configuration information associated with the first security sensor, and transmit data associated with the event signal to the remote server using the second communication interface, wherein the data associated with the event signal conforms with the configuration information associated with the first security sensor, the configuration information including an association between the first security sensor and at least one zone and an association of a response of the device with the at least one zone, the response including the interpreting the event signal and the transmitting the data.

2. The device of claim **1** further comprising:

a display coupled to the processor; and

the processor further configured to display data associated with the event signal using the display, wherein the data associated with the event signal conforms with the configuration information associated with the first security sensor.

3. The device of claim **1** further comprising:

an input device coupled to the processor; and

the processor further configured to receive, from the input device, configuration information associated with one or more of a security sensor, a monitoring device and an automation device, and store the received configuration information in the memory.

4. The device of claim **1** wherein the processor is further configured to:

receive, from the remote server via the second communication interface, configuration information associated with one or more of a security sensor, a monitoring device and an automation device; and

store the configuration information in the memory.

5. The device of claim **1** wherein the processor is further configured to:

read, from the memory, configuration information associated with one or more of a security sensor, a monitoring device and an automation device; and

transmit the configuration information to the remote server, using the second communication interface.

6. The device of claim 1 further comprising:

a third communication interface, coupled to the processor, for communication with the one or more monitoring devices; and

the processor further configured to generate configuration information associated with a first monitoring device of the one or more monitoring devices, configure the first monitoring device using an application programming interface associated with a type of the first monitoring device, and transmit, to the first monitoring device, the configuration information associated with the first monitoring device, using the third communication interface.

7. The device of claim 1 wherein the processor is further configured to:

couple among a third communication interface—and the processor for communication with the one or more monitoring devices;

receive, using the third communication interface, data from a first monitoring device of the one or more monitoring devices; and

transmit the data from the first monitoring device to the remote server, using the second communication interface.

8. The device of claim 1 further comprising:

a display coupled to the processor;

a third communication interface, coupled to the processor, for communication with the one or more monitoring devices; and

the processor further configured to receive, using the third communication interface, data from a first monitoring device of the one or more monitoring devices, in response to a request by a user of the device, and display, using the display, the data from the first monitoring device.

9. The device of claim 1 further comprising:

a third communication interface, coupled to the processor, for communication with the one or more monitoring devices; and

the processor further configured to transmit, using the third communication interface, control information to a first monitoring device of the one or more monitoring devices, wherein the control information conforms to configuration information associated with the first monitoring device.

10. The device of claim 1 further comprising:

a third communication interface, coupled to the processor, for communication with the one or more automation devices; and

the processor further configured to transmit, using the third communication interface, control information to a first automation device of the one or more automation devices, wherein the control information conforms to configuration information associated with the first automation device.

11. The device of claim 10 further comprising:

an input device coupled to the processor; and

the processor further configured to receive the control information from the input device.

12. The device of claim 10 wherein the processor is further configured to receive the control information from the remote server, using the second communication interface.

13. The device of claim 1, wherein the configuration information for the one or more security sensors comprises:

identification of a zone of a sensor of the one or more sensors;

identification of a type of the sensor;

identification of a unique identifier for the sensor; and

identification of a zone function for the sensor.

14. The device of claim 1 further comprising:

a display coupled to the processor;

the memory further storing instructions, executable by the processor, associated with one or more widget application programs and configuration information associated with the one or more widget application programs; and

the processor further configured to execute instructions associated with a first widget application program, and display information generated by the first widget application program using the display.

15. The device of claim 14, wherein the second communication interface is further configured to communicate with a remote portal server;

the one or more widget application programs are selected from a set of widget application programs using the remote portal server;

and the one or more widget application programs are distributed to the device by the remote portal server.

16. An apparatus comprising:

means for storing configuration information for one or more security sensors, configuration information for one or more monitoring devices, and configuration information for one or more automation devices;

first means for communicating with the one or more security sensors;

second means for communicating with a remote server;

means for interpreting an event signal received via the first means for communicating from a first security sensor of the one or more security sensors, wherein said means for interpreting performs said interpreting in accord with configuration information associated with the first security sensor; and

means for transmitting data associated with the event signal to the remote server using the second means for communicating, wherein the data associated with the event signal conforms with the configuration information associated with the first security sensor, the configuration information including an association between the first security sensor and at least one zone and an association of a response of the apparatus with the at least one zone, the response including the interpreting the event signal and the transmitting the data.

17. The apparatus of claim 16 further comprising:

means for displaying data associated with the event signal, wherein the data associated with the event signal conforms with the configuration information associated with the first security sensor.

18. The apparatus of claim 16 further comprising:

means for inputting configuration information associated with one or more of a security sensor, a monitoring device and an automation device.

19. The apparatus of claim 16 further comprising:

means for receiving from the remote server, via the second means for communicating, configuration information associated with one or more of a security sensor, a monitoring device and an automation device.

20. The apparatus of claim 16 further comprising:

means for reading, from the means for storing, configuration information associated with one or more of a security sensor, a monitoring device and an automation device; and

means for transmitting the configuration information to the remote server, via the second means for communicating.

21. The apparatus of claim **16** further comprising:
means for receiving data from a first monitoring device of the one or more monitoring devices; and
means for transmitting the data from the first monitoring device to the remote server, via the second means for communicating.

22. The apparatus of claim **16** further comprising:
means for transmitting control information to a first monitoring device of the one or more monitoring devices, wherein the control information conforms to configuration information associated with the first monitoring device.

23. The apparatus of claim **16** further comprising:
means for transmitting control information to a first automation device of the one or more automation devices, wherein the control information conforms to configuration information associated with the first automation device.

24. The apparatus of claim **16** further comprising:
means for storing instructions associated with one or more widget application programs and configuration information associated with the one or more widget application programs;
means for executing instructions associated with a first widget application program; and
means for displaying information generated by the first widget application program.

25. A method performed by a security, monitoring and automation controller, said method comprising:
storing configuration information for one or more security sensors, configuration information for one or more monitoring devices, and configuration information for one or more automation devices, wherein said storing is performed using a memory readable by the security, monitoring and automation (SMA) controller;
interpreting an event signal received from a first security sensor of the one or more security sensors, wherein said interpreting is performed in accord with configuration information associated with the first security sensor; and
transmitting data associated with the event signal to a remote server, wherein the data associated with the event signal conforms with the configuration information associated with the first security sensor, the configuration information including an association between the first security sensor and at least one zone and an association of a response of the SMA controller with the at least one zone, the response including the interpreting the event signal and the transmitting the data.

26. The method of claim **25** further comprising:
displaying data associated with the event signal, wherein said displaying is performed using a display coupled to the SMA controller, wherein the data associated with the event signal conforms with the configuration information associated with the first security sensor.

27. The method of claim **25** further comprising:
receiving, from the remote server, configuration information associated with one or more of a security sensor, a monitoring device and an automation device; and
storing the configuration information in the memory.

28. The method of claim **25** further comprising:
reading, from the memory, configuration information associated with one or more of a security sensor, a monitoring device and an automation device; and
transmitting the configuration information to the remote server.

29. The method of claim **25** further comprising:
generating configuration information associated with a first monitoring device of the one or more monitoring devices;
configuring the first monitoring device using an application programming interface associated with a type of the first monitoring device; and
transmitting the configuration information associated with the first monitoring device to the first monitoring device.

30. The method of claim **25** further comprising:
transmitting control information to a first monitoring device of the one or more monitoring devices, wherein the control information conforms to configuration information associated with the first monitoring device.

31. The method of claim **25** further comprising:
transmitting control information to a first automation device of the one or more automation devices, wherein the control information conforms to configuration information associated with the first automation device.

32. The method of claim **25** further comprising:
storing instructions, executable by the SMA controller, associated with one or more widget application programs, wherein said storing is performed using the memory;
storing configuration information associated with the one or more widget application programs, wherein said storing is performed using the memory; and
executing instructions associated with a first widget application program of the one or more widget application programs; and
displaying information generated by the first widget application program, using a display coupled to the SMA controller.

33. The method of claim **25** further comprising:
selecting the one or more widget application programs from a set of widget application programs, wherein said selecting is performed using a remote portal server coupled to the SMA controller; and
distributing the one or more widget application programs to the SMA controller by the remote portal server.

* * * * *